

5/19/05

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 837 383 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.04.1998 Bulletin 1998/17

(51) Int. Cl.⁶: G06F 1/00

(21) Application number: 97118074.0

(22) Date of filing: 17.10.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: 21.10.1996 JP 278423/96

(71) Applicant: FUJI XEROX CO., LTD.
Minato-ku, Tokyo (JP)

(72) Inventors:
• Saito, Kazuo,
c/o Fuji Xerox Co.,Ltd.
Ashigarakami-gun, Kanagawa (JP)

• Shin, Kilho,
c/o Fuji Xerox Co.,Ltd.
Ashigarakami-gun, Kanagawa (JP)
• Takeda, Koji,
c/o Fuji Xerox Co.,Ltd.
Ashigarakami-gun, Kanagawa (JP)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Method and apparatus for data verification

(57) A token 12 creates utilization history information and sends the information to an information processing unit 11 and simultaneously creates a verification value and stores the value in a utilization-value holding unit 21. The information processing unit 11 records the utilization history information in a history holding unit 16. On receiving a verification-value output request from the information processing unit 11, the token 12 provides the verification value with a signature and outputs the combination of the verification value and the signature. The information processing unit sends to a recovery unit 13 the verification value with the signature as well as the utilization history information. The recovery unit 13 verifies the signature and also the utilization history on the basis of the verification value further.

FIG.2

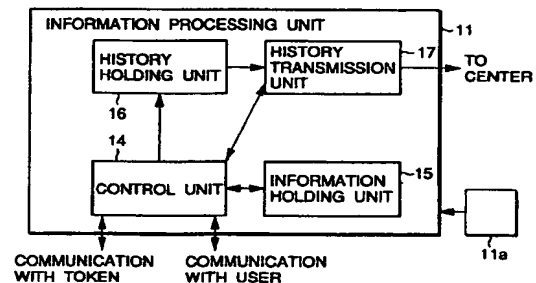
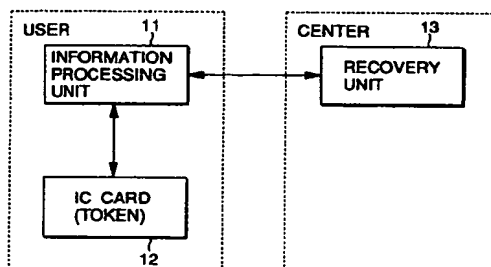


FIG.1



EP 0 837 383 A2

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the technology of verifying data and more particularly to data-verifying technology fit for use in general information processing units designed to transmit or hold a large continuous number of data groups, for example, a utilization history in security.

2. Description of the Related Art

With the recent progress of digital information processing technology, an idea of information highway and so forth, the time has come at last in that every sort of information is digitized, and the digital information is distributed and circulated through networks. The distribution and circulation of various kinds of information in the form of images, animations, voice, programs and the like, to say nothing of character information, have already been started via Internet, telecommunications-personal computer or in the form of CD-ROMs.

However, the digital information in the form of characters, images, animations, voice, programs and the like is of no value unless such information is utilized because it is different from physical matter and unsubstantial and easy to copy at low cost. Despite the features mentioned above, however, restrictions have been imposed on the copying of what is owned by someone once because one is to pay therefor at present. In other words, there is suspicion that easiness of copying and that easiness of copying at low cost that feature the digital information to the fullest extent are confined by arbitrary rules.

In order to solved the foregoing problems, there has recently appeared a system of making digital information utilizable by decrypting the information. More specifically, the digital information as represented by programs is encrypted so as to render the information freely distributable and when the information is utilized, each user receives a decrypting key after paying a price therefor. In view of the fact that information is of no value unless it is utilized, moreover, there has also been proposed a system of charging a payment for the utilization of information such as a software service system as disclosed in Japanese Patent Publication No. 95302/1994 and an apparatus for measuring the quantity of utilized information as disclosed in Japanese Patent Laid-Open No. 21276/1995.

With the aforementioned technologies, users are not asked to buy software when the software as represented by programs is utilized over personal computers and workstations but while they are able to acquire the software free of charge or at a moderate price, charged with a payment in proportion to the quantity utilized, for example, each time the software is utilized.

In order to charge a payment for the utilization of information, the charge has to be paid by each of the individual users, depending on the frequency of use. In a certain case, the charges collected in a lump have to be distributed to information providers in proportion to the frequency of use. Consequently, the utilization history in the user environment has to be recorded in security and also recovered in safety.

Nevertheless, though a utilization meter functioning as what records a utilization history has been mentioned in Japanese Patent Laid-Open No. 21276/1995, no reference has been made of how to recover the quantity of utilization actually recorded therein.

There has been proposed a method for the aforementioned purpose which is not to use a recording device under the control of an information processing device, for example, a hard disk with which the user utilizes the utilization history but to use an independent safety device. According to Japanese Patent Publication No. 95302/1994, for example, a utilization history is to be written to an IC card.

In a chargeable information transmitting system according to Japanese Patent Laid-Open No. 25605/1991 and a chargeable information collecting system according to Japanese Patent Laid-Open No. 180762/1994, chargeable information is recovered through networks.

When a history written to a safety device such as an IC card is recovered, there has been proposed a method of using a network or allowing a collector having a proper right to collect the history directly from such a device.

Under the method of collecting the history through the network, however, no consideration has been given to safety; the safety of chargeable information, that is, the possibility of falsification of chargeable information on the way, or otherwise the possibility of transmission of dishonest chargeable information from any one of the users. Therefore, the problem is that the aforementioned method remains unapplicable, in view of safety, to Internet open to the general public, though it is applicable to in-house networks that can be relied upon to a certain degree.

In order to safely recover the history in the form of an IC card in the apparatus, it has been the only way that a collector having a proper right to collect the history directly therefrom.

With the recent development of encrypting technology, however, the use of digital signature technology in particular

makes it possible to solve the aforementioned problem. More specifically, a private key peculiar to the safety device is enclosed therein and when a user wants to retrieve data from the safety device, the user is always called for providing a signature, whereby whether or not the data is right can be confirmed later by verifying the digital signature accompanying the data.

5 A technique of using RSA (Rivest-Shamir-Adleman) cryptosystem for digital signatures is widely known. However, signatures by means of RSA or any other digital signatures generally need a large quantity of calculations and so do a great deal of time per process normally. Therefore, a serious problem is posed when a signature has to be provided for continuous data in great quantities or when a computer with low calculating capability is used for processing signatures.

10 When the IC card is used as a safety device for recording the utilization history, the calculating capability of CPU mountable in such an IC card is often rather low in general and the problem is that a great deal of time is required when the CPU is used to carry out a large quantity of calculations. If, however, an attempt is made to increase the calculating capability in order to raise the calculating speed, this arrangement will become extremely costly.

There also exists a problem arising from a recording capacity when total data concerning the utilization history is recorded in a small device like the IC card because the data regarding the utilization history is usually of great length.

15 The security of modern encryption technology including the RSA is originally based on the quantity of calculations, and the length of the key used for a signature and cryptosystems is arranged so that it is increased as the capabilities of the computer increase. Consequently, this problem is not made solvable by only increasing the capabilities of a computer in future but still remains essentially to await a solution since use can be made of equipment (e.g., a personal token) only capable of employing a computer whose processing performance is far low in comparison with the highest performance that can be offered by the newest model of computer of the day.

SUMMARY OF THE INVENTION

25 An object of the present invention made in such circumstances as described above is to provide a method of making possible the creation of data verifiable at high speed even by an apparatus having low calculating capability.

More specifically, the total utilization history is not held in an IC card but only verification values obtainable from the utilization history are held in the IC card, and the utilization history proper is held on the part of an information processing unit (e.g., a personal computer or the like) to be controlled by a user.

30 Referring to the prior art in view of the verification values, there is technology employed for data communication, called DES-MAC. MAC is an abbreviation of Message Authentication Cryptosystem having a predetermined length showing that a message is complete (i.e., any message that has not been altered dishonestly). The cryptosystem is used after being attached to an original message. Since the occurrence of an error during the data communication is fatal, an arrangement is made so that a change in data during the data communication can be detected.

35 Further, DES is an abbreviation of Data Encryption Standard, which is a block encryption algorithm (Applied Cryptography pp 265) with 64 bits used for one block. A CBC (Cypher Block Chain) mode (Applied Cryptography pp 193, JIS-X5051) is one kind of way of using block cryptosystems as represented by DES, that is, a system of not encrypting an individual block independently but of exclusively ORing a block encrypted immediately before and a block to be encrypted next so as to make the value obtained a DES input. Even when blocks having the same contents under this system are encrypted and when the block that has been encrypted until then is different, the encrypted result will also become different.

40 The DES-MAC (Refer to Applied Cryptography pp 455 for CBC-MAC) is an application of the CBC mode in the DES, according to which the block obtained last is used for the verification value of the total data stream.

45 Fig. 21 shows an arrangement of DES-MAC. A stream of data to be transmitted is shown in the upper portion of Fig. 21 and the data stream is divided into blocks each having 64 bits. IV is an abbreviation of Initial Vector representing an initial value formed of random numbers. The blocks resulting from the division are passed in a chain through DES encryptors as in the DES-CBC mode by adding IV to the head of the data stream and the block obtained last to the last position thereof as the verification value of the data stream for transmission. On the reception side, a verification value is obtained by performing the process in reverse order and compared with the value received for verification.

50 The processing method like this is basically intended for data transmission by means of communication. Since a sender sets it forth as a premise to hold complete data in a short time with certainty, there will develop a problem if the premise is applied to the recovery of a complete history. This is because history data are accumulated over a long period of time, during which the data may arbitrarily be controlled by users or the system may have accidents and thus be exposed to danger.

55 To begin with, the aforementioned system (DES-MAC) is based on the assumption that the data blocks are continuously transmitted. In other words, for the transmission of ordinary data, there exists a lower layer (equivalent to a TCP layer in TCP/IP: transmission control protocol/Internet protocol) and the order of data blocks is assured by that layer.

If, however, the utilization history is put under the control of the user, the order of histories becomes unassured at that point of time; that is, the user is allowed to use the IC card by connecting it to a plurality of computers (e.g., a desk

top PC, a lap top PC, etc.) that the user can use. When it is into consideration that the utilization history is recorded on the computer side, the utilization history is scattered in the plurality of computers. Consequently, the history thus scattered in the plurality of computers is deprived of the order in terms of time.

In the case of a utilization history, the time order is an extremely important factor. In other words, the usage may be calculated later from the plurality of continuous histories. For example, there are cases; namely, a simple case where utilization time is calculated from the difference between utilization start time and utilization end time; another case where the usage is determined by calculating a difference in data length from data length as an object of operation at the utilization start time and from data length as an object of operation at the utilization end time; and so forth.

The DES-MAC has furnished no substantial solutions to the foregoing problems.

A further problem arising when the utilization history is put under the control of the user is that part of the utilization history may be lost intentionally or by accident. In the case of DES-MAC, verification will become impossible if part of the utilization history is lost. Since the DES-MAC is based on the assumption that the sender holds complete data only during the communication, carrying out retransmission will settle the case. However, the loss of the utilization history means the substantial loss of data and therefore the restoration of the history becomes impossible. The still continuous use of the DES-MAC system makes infeasible even the verification of the remaining data.

In a system of charging a payment for the usage, further, it is prerequisite for the user to recover the history left on hand. Unless the history is recovered, there will develop a problem of rendering uncalculable the utilization fee charged against the user or otherwise rendering the collected utilization fee undistributable to information providers.

Thus, the utilization history left with the user has to be recovered safely and to this end, it is avoided that the utilization history is recovered under false recovery instructions.

An object of the present invention is therefore to provide an apparatus capable of verifying lengthy data quickly even with its low calculating capability and small storage capacity.

Further, a second object of the present invention is to provide a method of making data order restorable even in such an environment that the order is not preserved.

Further, a third object of the present invention is to provide a method of making the remaining data verifiable even when part of the data is lost.

Further, a fourth object of the present invention is to provide a method of controlling a data-holding apparatus safely from the outside.

In order to solved the foregoing problems according to the present invention, basically data is not recorded in a protective apparatus to reduce the quantity of data to be held but output from the protective apparatus outside and verification values small in data quantity are held in the protective apparatus instead. More specifically, unidirectional functions in place of digital signatures are used for verification so that data may be verified quickly. When hash functions representing MD5 are realized in software, hash values are said to result in proving that they are higher in speed by three digits than the encrypting process of RSA. In order to make the order of history data restorable, further, restorable information is added to the order of history data. More specifically, it has been arranged that the value provided with a signature of a right person is necessitated with respect to the verification value held by the protective apparatus, whereby the verification value in the protective apparatus is forcibly sent to the right person to ensure that the verification is effected.

A description will subsequently be given of the constitution of the present invention. In order to accomplish the objects above according to the present invention, a data verifying method comprises the steps of: creating a verification value of a data body inside a protective apparatus from a verification value of the relevant data body out of a plurality of data bodies generated in sequence and a verification value of a data body preceding the relevant data body, creating a verification value with a signature by adding a digital signature inside the protective apparatus to the verification value created for the last data body out of the plurality of data bodies to be verified at a time, sending the verification value with the signature outside from the protective apparatus, and verifying the plurality of data bodies based on the plurality of data bodies and the verification value with the signature.

With this arrangement, it is only needed to provide the verification value with the digital signature even though the calculating capability is low. Since the verification can be calculated from the verification value with respect to the preceding data body and the data body this time, the processing is performable as long as one data body and one verification value are holdable, which means the storage capacity may be small.

In order to accomplish the objects above according to the present invention, further, an apparatus for creating data to be verified is provided with: means for generating data bodies in sequence, verification value holding means for holding verification values, verification value creation means for creating a new verification value from the verification value held in the verification value holding means and a newly generated data body and updating the verification value held in the verification value holding means to the new verification value, and signature means for attaching a signature to the verification value held in the verification value holding means at predetermined timing, wherein the verification value creation means, the verification value holding means and the signature means are installed in a protective apparatus.

Even with this arrangement, it is only needed to provide the verification value with the digital signature even though

the calculating capability is low. Since the verification can be calculated from the verification value with respect to the preceding data body and the data body this time, the processing is performable as long as one data body and one verification value are holdable, which means the storage capacity may be small.

In order to accomplish the objects above according to the present invention, further, there are provided a plurality of data bodies generated in sequence, means for receiving a verification value with a signature resulting from providing a signature for the verification value calculated from the plurality of data bodies, signature verifying means for verifying the signature on the verification value received, and verifying means for verifying the correctness of the plurality of data bodies received from the verification value with the signature verified by the signature verifying means.

With this arrangement, the quantity of calculations is reducible since the verification of the signature is effected for only the verification value with the signature.

In order to accomplish the objects above according to the present invention, further, a history holding method is used for holding in a protective apparatus only a verification value resulting from sequential calculations with respect to a group of history data comprising a plurality of continuous history data, and providing a signature for only the verification value when the verification value is output from the protective apparatus outside.

With this arrangement, not only the quantity of calculations but also the storage capacity can be suppressed.

In order to accomplish the objects above according to the present invention, further, a history holding apparatus is provided with: data input means for inputting a plurality of continuous data, data processing means for processing the data, verification value creation means for creating a verification value with history data relevant to the data processing and the verification value held at this point of time as inputs, verification value holding means for holding the verification value thus created, and signature means for providing a signature for the verification value, wherein the verification value creation means, the verification value holding means and the signature means are at least installed in a protective apparatus.

With this arrangement, not only the quantity of calculations but also the storage capacity can be suppressed.

With this arrangement likewise, unidirectional functions may be used for calculations applicable to the verification value creation means. The history data may be in the form of a combination of the history data body and the verification value at the time the history data is processed. Further, counter means for doing counting each time data is processed may be provided and the history data in the history data group may be in the form of a combination of the value of the counter when the data is processed and a history body. The verification value with the signature may be output in compliance with a user's request. The history holding means may comprise a single CPU with software and when the load of the CPU applied by the data processing means is low, the signature means may create and outputs the verification value with the proper signature.

With this arrangement, further, function stopping means may be provided and used for stopping the function of the data processing means at a point of time the verification value is output until a proper instruction is given from the outside. Halt condition holding means may be provided and used for stopping the function and when the conditions described in the halt condition holding means are met, the function halt means may output the verification value with the signature written thereto and stop its function. Further, proper public-key holding means may be used for holding a public key of an external right person, and the function halt means may verify that an accepting instruction is intended to restore the function corresponding to the lastly-output verification value provided with a digital signature made by the external right person and that by verifying the signature with the public key held by the proper public-key holding means at the time of receiving the instruction, whether or not the verification value with the signature is equal to the verification value held by the verification value holding means.

In order to accomplish the objects above according to the present invention, further, a history verifying apparatus may be provided with: data input means for inputting a verification value with a signature, the signature being provided for the verification value calculated from a plurality of continuous history data in group and from the data groups, signature verifying means for verifying the signature of the verification value thus received with the signature, and verifying means for verifying the correctness of the data group received from the data group received and the verification value whose signature has been verified.

With this arrangement, the quantity of calculations is reducible since the verification of the signature is effected for only the verification value with the signature.

With this arrangement, further, previous verification value storage means may be provided and used for storing the verification value received the last time, and the verifying means may employ the previous verification value when making verification. The calculations for use in the verifying means may be based on unidirectional functions. The history data may be in the form of a combination of the history data body and the verification value at the time the history data is processed. The history data in the history data group may be in the form of a combination of the value of the counter when the data is processed and a history body.

In order to accomplish the objects above according to the present invention, further, a history holding apparatus may be provided with: data storage means for holding data, halt condition holding means for holding predetermined conditions at the time the function is stopped, function halt means for stopping the function when the conditions held in

the halt condition holding means are met and keeping the function stopping until a proper instruction is received from the outside, private-key holding means for holding a private key, digital signature means for providing a digital signature using the private key held in the private-key holding means for the data group held in data holding means, digital signature holding means for holding the digital signature affixed, and proper public-key holding means for holding the public key of an external right person, wherein the function halt means may verify that an accepting instruction is intended to restore the function corresponding to the digital signature provided by the external right person for the digital signature held in the digital signature holding means and that by verifying the signature with the public key held by the proper public-key holding means at the time of receiving the instruction, whether or not the value with the signature is equal to the value held by the digital signature holding means.

With this arrangement, the instruction with the signature of the proper person is not sent until the correctness of the history is verified, and the halt state of the apparatus is not release not until the correctness of the instruction is verified. Therefore, no inconvenience arises from the provision of service while the correct history remains unrecovered. In other words, it is ensured that the correct history is recovered.

According to the present invention, electronic equipment is provided with: function halt means for stopping at least part of the function of an electronic equipment body when predetermined conditions are met, means for outputting predetermined data outside, means for receiving data with a signature, the data being created by providing the signature for the predetermined data, signature verifying means for verifying the signature with respect to the data with the signature, and means for releasing the halt state of that part of the function when the correctness of the signature of the data with the signature is verified by the signature verifying means.

With this arrangement, the use of the electronic equipment is not made to continue until the correctness of the data is verified, so that correct data is secured.

Further, the present invention can be implemented by appropriating part thereof to a computer program product.

The above and other objects and features of the present invention will be more apparent from the following description taken in conjunction with the accompanying drawing.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an overall block diagram of Embodiment 1 of the present invention;

Figure 2 is a block diagram showing the construction of an information processing unit 11 of Fig. 1;

Figure 3 is a block diagram showing the construction of a token 12 of Fig. 1;

Figure 4 is a diagram explanatory of a utilization-value holding unit 21 of Fig. 3;

Figure 5 is a block diagram showing the construction of a recovery unit 13 of Fig. 1;

Figure 6 is a diagram explanatory of information to be decrypted in the token 12;

Figures 7A and 7B are diagrams explanatory of the construction of a utilization history;

Figure 8 is a flowchart explanatory of processing to be performed in the control unit 14 of the information processing unit 11 when a request for the utilization of information is received from a user;

Figure 9 is a flowchart explanatory of processing to be performed in the control unit 14 of the information processing unit 11 when an instruction for the recovery of the utilization history is received from a user;

Figure 10 is a flowchart explanatory of processing when the decryptor unit 19 of the token 12 receives a request for decrypting encrypted information from the information processing unit 11;

Figure 11 is a flowchart explanatory of processing to be performed in the utilization-value creating unit 20 of the token 12 which is called from the decryptor unit 19 of the token 12;

Figure 12 is a flowchart explanatory of processing when the utilization-value output unit 22 of the token 12 receives a verification-value output request from the information processing unit 11;

Figure 13 is a block diagram showing the construction of the token 12 in Embodiment 2;

Figure 14 is a flowchart explanatory of processing to be performed in the token 12 of Fig. 13;

Figure 15 is a flowchart explanatory of processing to be performed in the token 12 of Fig. 13;

Figure 16 is a flowchart explanatory of processing to be performed in the token 12 of Fig. 13;

Figure 17 is a block diagram showing the function block materialized in the information processing unit 11 in Embodiment 2;

Figure 18 is a block diagram showing the construction of the recovery unit 13 in Embodiment 2;

Figures 19A to 19E are diagrams showing the construction of the utilization history in Embodiment 2;

Figure 20 is a diagram explanatory of another construction of the utilization history in Embodiment 2; and

Figure 21 is a diagram explanatory of relevant technology.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Now, a description will be given in more detail of preferred embodiments of the invention with reference to the

accompanying drawings.

(Embodiment 1)

Embodiments of the present invention will subsequently be described. First, Embodiment 1 of the present invention will be described. In a system to be described in Embodiment 1 of the present invention like any other systems according to the present invention as those which will be described later, general digital information such as programs and image information that are encrypted and distributed is utilized in an information processing unit like a personal computer or a workstation by means of an IC card (hereinafter called the "token") connected to the information processing unit in order to record the utilization history then by seizing timing at which the information is decrypted, whereby to make the center recover the utilization history. Needless to say, the present invention is applicable to any task other than securing history data.

Fig. 1 shows an overall system configuration according to this embodiment of the invention. In Fig. 1, there is shown an information processing unit 11 like a personal computer or a workstation for use in utilizing digital information in the user environment and in order to decrypt encrypted information (or to decrypt a key for decrypting, a token 12 for recording the utilization history by seizing the timing is connected to the information processing unit. The token 12 and the information processing unit 11 may be connected via any means capable of transmitting information such as a PC card (PCMCIA: Personal Computer Memory Card Interface Association) interface, serial/parallel, an infrared ray and the like. The token 12 may be packaged in the information processing unit 11.

The user's information processing unit 11 is connected to a recovery unit 13 constituted of an information processing unit such as a workstation or a large computer on the center side. The connection may be in the form of a modem-to-telephone line or a network interface like Ethernet. The connection is not maintained at all times and may be made only when the recovery of the utilization history from the user's information processing unit 11.

Fig. 2 shows the construction of the information processing unit 11 on the user side. The user's information processing unit 11 may be a personal computer or a workstation for general use. The only difference is that the token 12 is connected to the information processing unit 11. The information processing unit 11 includes a control unit 14, an information holding unit 15, a history holding unit 16 and an information transmission unit 17. With this arrangement, a recording medium 11a stored with a program, for example, is used to install the program.

While communicating with the token 12, the control unit 14 performs the following processes including:

- (1) reading the encoded information stored in the information holding unit 15, transferring the information to the token 12 for decrypting purposes and executing or processing the information;
- (2) receiving the utilization history transferred from the token 12 simultaneously when the decrypted data is received and storing the utilization history in the history holding unit 16; and
- (3) issuing a "verification value output" command to the token 12 on receiving an instruction from the user and transferring the utilization history provided with a digital signature to the information transmission unit 17.

The information holding unit 15 is stored with data, information or decrypted data to be utilized by the user. Actually, the information holding unit 15 is formed with an external storage device like a memory or a hard disc device.

The history holding unit 16 is stored with the history transferred from the token 12 via the control unit 14. Actually, the history holding unit 16 is formed with an external storage device like a memory or a hard disc device. The specific construction of a history will be described later.

On receiving the command from the control unit 14, the information transmission unit 17 reads out the history held in the history holding unit 16 together with the utilization history transferred from the control unit 14, and transmits the history to the recovery unit 13 of the center. The information transmission unit 17 is actually constituted of a modem and a telephone line or a network interface such as Ethernet. However, a device such as a floppy disc instead of Ethernet is used to store the data, so that the user may manually input it to the recovery unit 13 of the center.

Fig. 3 shows the construction of the token 12 on the user side. The token 12 is physically and generally constituted of MPU, a memory and the like. The token 12 itself is contained in a container resistant to a physical attack from the outside. Since the attach-resistant container is technologically well known (Japanese Patent No. 1860463, Japanese Patent Laid-Open No. 100753/1991, etc.), the description thereof will be omitted. To what extent the container is resistant varies with the degree of security of the data involved. There is a case where the preparedness for such an attack may be weak.

The token 12 is connected to the user's information processing unit 11, performs predetermined processing according to an instruction from the information processing unit 11 and returns the result thereto. The token 12 comprises a user private-key holding unit 18, a decryptor unit 19, a utilization-value creating unit 20, a utilization-value holding unit 21, a utilization-value output unit 22, a token private-key holding unit 23, a digital signature unit 24 and so forth. Each of the components of the token 12 will be described later. The token 12 has the following functions:

(1) Information decrypting function with holding of the utilization history including:

- (i) receiving encrypted data from the information processing unit 11, decrypting the data with the private key stored in the user private-key holding unit 18, and returning the decrypted data to the information processing unit 11;
- (ii) performing the decrypting process simultaneously with referring to the header of the decrypted data and the identifier written thereto, and returning the identifier to the information processing unit 11 as the utilization history; and further
- (iii) transferring the utilization history to also utilization-value creating unit 20, and causing the utilization-value creating unit 20 to make calculations with respect to the utilization history and the verification value held in the utilization-value holding unit 21 at that point of time.

(2) Verification value output function including:

- providing a digital signature for the verification value held in the utilization-value holding unit 21 at that point of time on receiving an output request from the information processing unit 11, returning the verification value with the signature thereto, and erasing the data in the utilization-value holding unit 21.

A description will subsequently be given of each components of the token 12.

In response to a decrypting request from the information processing unit 11, the decryptor unit 19 performs the decrypting process using a private key peculiar to the user held in the user private-key holding unit 18 and returns the result to the information processing unit 11 as encrypted data. At this time, the decryptor unit 19 simultaneously read the header of the encrypted data, returns the information identifier written thereto to the information processing unit 11 as the utilization history and also to the utilization-value creating unit 20 (in this example, the information identifier of the information utilized is used for the utilization history).

With the arrangement like this, the user needs to gain access whenever utilizes information, so that the utilization history is recorded without fail.

In this case, the encrypted data transferred from the information processing unit 11 may be what is formed by encrypting information itself or a key for decrypting the encrypted information. In the case of the latter, the process of decrypting the information proper is performed on the side of the information processing unit 11.

The user private-key holding unit 18 holds a private key peculiar to the user. Generally, tokens 12 are distributed to users in such a form that a key peculiar to each user is enclosed beforehand at the token issuing center. Therefore, the user's private key remains unknown to the user himself.

The utilization-value holding unit 21 holds only one verification value which is updated in sequence. Generally, the verification value is a value having a fixed length of 16 bytes or the like. If a verification value has 16 bytes, only a memory of 16 bytes is employed, Fig. 4 shows an example of the formation of such a verification value.

On receiving a verification value output request from the information processing unit 11, the utilization-value output unit 22 functions as what reads the verification value stored in the utilization-value holding unit 21 at that point of time and returns the verification value to the information processing unit 11. At that time, the utilization-value output unit 22 calls the digital signature unit 24 and provides a digital signature for the verification value.

The digital signature unit 24 uses the private key held in the token private key holding unit 23 for holding a special private key for the token to perform the process of providing a digital signature for the given value. The token private key holding unit 23 is a constituent unit for holding the private key for the purpose of signature used when a digital signature is made. For these constituent units, it is possible to use digital signature technology such as RSA signature, of which the description will be omitted because it belongs to the prior art.

On receiving the utilization history (the information identifier in this case) from the decryptor unit 19, the utilization-value creating unit 20 reads the verification value held in the utilization-value holding unit 21 and calculates a new verification value from the utilization history and the verification value by making the following calculation.

$$H = \text{Hash} (\text{Usage} + \text{Hold}) \quad [\text{Numerical Formula 1}]$$

where H = new verification value, Hold = the present verification value, Usage = utilization history and Hash () = unidirectional function, MD and SHA (Secure Hash Algorithm) being actually employed. In this operation "+", numerical values may actually be added up or exclusively ORed on condition that both have the same length or otherwise two data may simply be arranged in order; in any one of the above cases, it is essential for the two values are synthesized. The utilization-value creating unit 20 stores the new verification value thus calculated in the utilization-value holding unit 21 (e.i., the new value is superscripted).

On receiving the output request from the information processing unit 11, the utilization-value output unit 22 returns

the verification value held in the utilization-value holding unit 21 at that point of time and resets the utilization-value holding unit 21 to a predetermined value or may simply clear the verification value thus held therein.

The recovery unit 13 of the center will subsequently be described. Fig. 5 shows the construction of the recovery unit 13. As shown in Fig. 5, the recovery unit 13 comprises a history reception unit 25, a history holding unit 26, a history verification unit 27, a token public-key holding unit 28, a signature verification unit 29 and so forth. The recovery unit 13 causes the history reception unit 25 to receive the history sent from the information processing unit 11 of the user and stores the contents in the history holding unit 26. The utilization history stored is read by the history verification unit 27 where it is verified whether or not the history is correct, and then the verified result is sent to an administrator on the center side.

Then the center normally calculates information utilization fees in accordance with the contents of the history, collects the fees from users and performs the process of distributing the utilization fees thus collected among information providers according to details of an information utilization history. However, the description of this matter will be omitted because it is irrelevant to the essence of the present invention.

A description will subsequently be given of each of the components of the recovery unit 13.

The history reception unit 25 receives the history information sent from the information processing unit 11. Actually, like the history transmission unit 17 of the information processing unit 11 (Fig. 2), the history reception unit 25 is constituted of a modem and a telephone line or a network interface such as Ethernet or an information input device from the outside such as a floppy disc. The utilization history received by the history reception unit 25 is stored in the history holding unit 26.

In order to verify whether the verification value sent from the information processing unit 11 is correct, further, there are provided the token public-key holding unit 28 and the signature verification unit 29.

When a history is transmitted from the information processing unit 11, the history reception unit 25 receives the history. The history thus received is stored in the history holding unit 26 and transferred to the signature verification unit 29. The signature verification unit 29 selects the public key of the token 12 connected to the information processing unit 11 that has sent the history from among the public keys of the plurality of tokens 12 stored in the token public-key holding unit 28, and verifies the signature of the history using the public key. The verified result is held together with the history stored in the history holding unit 26. When the verified result is proved to be false, processing thereafter is discontinued since there is some possibility that the verification value has been altered dishonestly or fabricated and the administrator outputs to that effect and stops the processing.

When the signature is verified, the following processing is continued:

The history holding unit 26 holds the utilization history transferred from the history reception unit 25 and the verified result. The history holding unit 26 is actually formed of a storage device such as a memory.

The history verification unit 27 verifies the history held in the history holding unit 26 as follows:

- (1) A series of histories transmitted are defined as $ud_1, ud_2, ud_3 \dots ud_n$;
- (2) The verification value attached to the last position of the history is defined as hud ; and
- (3) Provided the initial value of the verification value is defined as $ihud$, it is examined whether hud' resulting from calculation becomes equal to the hud sent according to the following expression:

[Numerical Formula 2]

$$hud' = Hash(ud_n + Hash(ud_{n-1} + \dots Hash(ud_2 + Hash(ud_1 + ihud)) \dots))$$

$$hud = ?hud'$$

- (4) If the equation is established, the verification value is judged that it has not been altered dishonestly but if not, it has been altered. The administrator of the recovery unit is then informed of the result.

A description will subsequently be given of the form of information to be processed in each unit.

Fig. 6 shows a form of encrypted information as an object of encrypting in the token 12: (a) refers to a case where information itself is encrypted with a user's private key; and (b) to a case where the private key used for initially encrypting the information proper is encrypted by a private key peculiar to the user before being decrypted and the private key peculiar to the information thus obtained is used for decrypting the information proper. In the case of (b), the information

proper may be decrypted by the information processing unit, not by the token 12. Further, a public key may needless to say be used, though a description has been give of an example using a common cryptosystem.

The information identifier is an identifier peculiar to the information given when the center encrypts the information for distribution. The information identifier is controlled by the center (e.g., with a database) and when the information identifier is specified, it is possible to specify a person who has prepared the information, for example.

Figs. 7A and 7B show a form of utilization history: Fig. 7A shows a form of the utilization history recorded in the information processing unit 11 according to this embodiment of the invention, that is, a train of information identifiers (the information decrypted by the token) utilized; and Fig. 7B shows a form of the utilization history sent from the information processing unit 11 to the center, this form differs from that of Fig. 7A solely in that the verification value held by the token and the signature of the token with respect to the verification value are attached to the last position of Fig. 7A.

Although the individual utilization history is constituted of only the information identifiers utilized according to this embodiment of the invention, it may include any data, for example, utilization time, the identifier of the user, the quantity of utilization, an utilization fee and so on. In other words, the present invention is effective when various kinds of information are left as a history (various kinds of information are usually left as a history) since the individual history tends to become long.

Referring to Figs. 8 - 12, there will be given a description of processing performed in the information processing unit 11 and the token 12. Fig. 8 refers to a processing flow when a request for the utilization of information is made from a user in the control unit 14 of the information processing unit 11. Fig. 9 refers to processing when an utilization history recovery instruction is given by the user in the control unit 14 likewise. Fig. 10 refers processing when the decryptor unit 19 of the token 12 receives a request for decrypting the encrypted information from the information processing unit 11. Fig. 11 refers to processing in the utilization-value creating unit 20 of the token 12 when called by the decryptor unit 19 of the token 12. Fig. 12 refers to processing when the utilization-value output unit 22 of the token 12 receives a verification-value output request from the information processing unit 11.

As shown in Fig. 8, the following processing proceeds in the control unit 14 of the information processing unit 11 when a request for the utilization of information is made from the user. First, a decision is made on whether the intended information has been encrypted (S11). If not encrypted yet, the information as it stands is processed (S15). If already encrypted, a decrypting request is made to the token 12 so as to transfer the intended information (S12). When an error is returned from the token 12, the processing is terminated after issuing an error message "the history of the token is full" (S13, S16). If no error is returned, the utilization history fed from the token 12 is recorded in a recording unit such as a disc (S14). Then the intended information is processed (S15).

As shown in Fig. 9, the following processing proceeds in the control unit 14 of the information processing unit 11 when the utilization history recovery instruction is given by the user. First, a decision is made on whether the intended information has been encrypted (S21). If not encrypted yet, the information as it stands is processed (S24). If already encrypted, the decrypting request is made to the token 12 so as to transfer the intended information (S22). Then the utilization history returned from the token 12 is recorded in the recording unit such as a disc (S23). Thereafter, the intended information is processed (S24).

As shown in Fig. 10, the following processing proceeds when the decryptor unit 19 of the token 12 receives a request for decrypting the encrypted information from the information processing unit 11. First, a user private key K_u is taken out from the user private-key holding unit 18 (S31). The encrypted data is decrypted with the user private key K_u and the decrypted data is stored (S32). The header of the decrypted data is referred to so as to read an information identifier and with this identifier as a subtraction number, the utilization-value creating unit 20 is called and made to perform verification-value creating process (S33, S34, see Fig. 11). Then the decrypted data and the identifier are sent back to the information processing unit 11 (S35).

As shown in Fig. 11, the following processing proceeds when the utilization-value creating unit 20 of the token 12 receives a call from the decryptor unit 19 of the token 12. First, the verification value is taken out from the utilization-value holding unit 21 (S41). The information identifier and the verification value are subjected to hash calculation, and the calculated result is stored in the utilization-value holding unit 21 as a new verification value (S42, S43).

As shown in Fig. 12, the following processing proceeds when the utilization-value output unit 22 of the token 12 receives the verification-value output request from the information processing unit 11. First, the verification value stored in the utilization-value holding unit 21 is read out (S51). Then the contents stored in the utilization-value holding unit 21 are initialized (S52). With the verification value thus read as a subtraction number, the digital signature unit 24 is called so as to provide the verification value with a signature (S53). The signature is affixed to the last position of the verification value, and the verification value with the signature is output (S54).

The description of Embodiment 1 is terminated for the moment.

In a case where a user verifying apparatus and method as disclosed in Japanese Patent Application No. 62076/1996 are combined with the present invention, modulo n can be used as an information identifier by varying the modulo n in the calculation of power residue each time an access ticket is issued. More specifically, in the user verification technique of Japanese Patent Application No. 62076/1996, the access ticket (auxiliary information for verification)

is received from the outside, so that encrypted data, for example, is decrypted by the use of the access ticket and the user verification information. Further, the modulo n used then is used as an information identifier. In this case, the modulo n is not taken out before being decrypted by the decryptor unit inside the token but given from the outside together with information as an object of encrypting.

With this arrangement, the capacity of the utilization-value holding unit 21 that has to be prepared within the token 12 can be minimized and thereby the production cost of the token 12 is also made reducible.

(Embodiment 2)

Embodiment 2 of the present invention will subsequently be described. Embodiment 2 described herein has several functions in addition to those in Embodiment 1. The functions and effects will be enumerated as follows:

(1) The token 12 outputs the verification value and stops its function but recovers the function on receiving a message from the center.

When the verification value is output outside or when a predetermined time is passed by the use of a clock function, the token 12 outputs the verification value and stops at that point of time to urge the user to recover the history (or may autonomously stop so as to demand a verification value). In order for the user to have the function of the token 12 recovered, the only way is to send the history and the verification value to the center for verifying purposes and to receive a message for use in recovering the function from the center. The message issued by the center for the purpose of recovering the function is formed by providing the verification value sent from the user with the digital signature added by the center.

(2) The verification value is also output at a point of time the utilization history as its history is processed.

Not only the information identifier but also the verification value at the point of time the history is generated is contained in the contents of the utilization history, whereby strict control of the history (order) on the information processing unit side can be dispensed with since the continuity of the individual history is made examinable.

(3) An old verification value is held on the center side.

In the embodiments of the present invention up to now, the verification value within the token has been initialized in compliance with the output request from the user. However, this function can be dispensed with by making the recovery unit of the center hold the preceding verification value of the user.

Fig. 13 shows the construction of the token 12 according to this embodiment of the invention, wherein like reference characters designate like or corresponding parts of Fig. 3 and the detailed description thereof will be omitted. As shown in Fig. 13, the token 12 comprises the user private-key holding unit 18, the decryptor unit 19, the utilization-value creating unit 20, the utilization-value holding unit 21, the token private key holding unit 23, the digital signature unit 24, a control unit 30, a history creating unit 31, a calculating unit 32, a center public-key holding unit 33, a signature verification unit 34 and so forth. A clock unit 35 may be provided, if necessary.

It is arranged according to this embodiment of the invention that communication with the information processing unit 11 is totally conducted via the control unit 30, which properly calls any other processing unit and performs processing in compliance with a request from the information processing unit 11.

The control unit 30 holds the operating state of the token 12 therein, the operating state being divided into two: a normal and a halt mode. In the normal mode, the token 12 performs the decrypting process as described in Embodiment 1 in compliance with a decrypting request from the information processing unit 11. In the halt mode, on the other hand, the token 12 accepts no decrypting request but basically only a function restart request (verification value with the signature made by the center). The token 12 cancels the halt mode when the request is rightful and performs the process of transferring the halt mode to the normal mode (in addition, may also actually perform the process of outputting a verification value resulting from providing a signature for the verification value held in the utilization-value holding unit 21 at that point of time).

Transferring the normal mode to the halt mode depends on the number of times the decrypting process, for example, is performed. The calculating unit 32 of Fig. 13 holds the number of times the decrypting process is performed. When that number of times exceeds a predetermined value (e.g., 100 times), for example, the control unit 30 returns a message "the time limit expired" to the information processing unit 11 and restores the halt mode.

When a clock is installed, information as to the preceding halt time held within the control unit 30 may be relied upon. In other words, on receiving a request from the information processing unit, the control unit compares the preceding halt time held in the control unit with the present time and returns the message "the time limit expired" to the information processing unit 11 when a predetermined period of time has passed (e.g., one month), and restores the halt mode.

Referring to Figs. 14 - 16, there will be given a detailed description of processing to be performed by the control unit 30 of the token 12. Incidentally, the parts shown with dotted lines in Figs. 14 - 16 represents not the process steps taken

by the control unit 30 but those taken by relevant constituent units.

In Fig. 14, one of the encrypting, verification-value output and function restart requests are input to the control unit 30 of the token 12 from the information processing unit 11. First, a decision is made on whether the mode of the control unit 30 is the halt mode (S61). Unless the halt mode is established, a count in the calculating unit 32 is read and a decision is made on whether the count exceeds, for example, 100 (S62, S63). If the count does not exceed 100, the flow proceeds to a node B of Fig. 16 where the decrypting process is performed. When the count exceeds 100, a verification value with a signature is output. In other words, a value in the utilization-value holding unit 21 is read out and the digital signature unit 24 is caused to create the verification value with the signature, which is output (S64, S65). Then the verification value with the signature and a message "transfer to the halt mode" are returned to the information processing unit 11 (S66). Further, the count in the calculating unit 32 is cleared and the halt mode is restored (S67, S68).

When the control unit 30 is in the halt mode at Step S61, a decision is made on whether the request received is the encrypting request, the verification-value output request or the function restart request (S69, S70, S71). When the request is the encrypting request, a message "the halt mode at present" is returned to the information processing unit 11, and the processing is terminated (S72). When the request is the verification-value, the verification value in the utilization-value holding unit 21 is read out and the digital signature unit 24 is caused to create the verification value with the signature, which is output (S73, S74). Then the verification value with the signature is returned to the information processing unit 11, and the processing is terminated (S75). When the request is the function restart request, the function restart process at a node A is followed. When the request received is not the encrypting request, the verification-value output request nor the function restart request, an error is returned to the information processing unit 11, and the processing is terminated (S76).

Fig. 15 shows the function restart process. In Fig. 15, the received verification value with the signature is delivered to the digital signature unit 24 so as to verify the correctness of the signature (S77). If the signature is correct, the verification value thus delivered is compared with the verification value in the utilization-value holding unit 21 and examined whether both conform to each other (S78 - S80). If both conform to each other, the mode of the control unit is transferred from the halt mode to the normal mode, and a message "function restart" is returned to the information processing unit 11 (S81, S82). If the signature is incorrect at Step S78, a message "incorrect signature" is returned to the information processing unit 11, and the processing is terminated (S83). When the verification value is inconsistent at Step S80, a message "inconsistent verification value" is returned to the information processing unit 11, and the processing is terminated (S84).

Fig. 16 refers to a case where the count does not exceed a threshold value, for example, 100. In Fig. 16, whether or not the request is the encrypting request is inspected (S85). When it is the encrypting request, the delivered data is sent to the decryptor unit 19 (S88). The decryptor unit 19 carries out the encrypting operation (S89 - S93). When the request is not the encrypting request, a decision is made on whether it is the verification-value request (S86). When it is the verification value request, the flow proceeds to a node C of Fig. 14 where the verification-value output process is performed. When the request is not the verification-value output request at Step S86, an error is returned to the information processing unit 11, and the processing is terminated (S87).

The description of the processing in the control unit 30 of the token 12 is terminated for the moment.

Although it has been arranged to restore the halt mode even when the verification value request is made from the information processing unit 11 according to this embodiment of the invention (transferring from Step 86 of Fig. 16 to the node C of Fig. 14), this arrangement need not necessarily be made. With respect to the verification value request in the normal mode, for example, the verification value is updated and then a signature is provided for the verification value held at that point of time so that the then value may be returned (this merit will be described at the end of the description of this embodiment of the invention).

The decryptor unit 19 and the user private-key holding unit 18 have the same functions as those described in Embodiment 1 of the present invention.

The history creating unit 31 performs, as also shown in Fig. 16, the process of generating three sets of the information identifier delivered from the decryptor unit 19 and the present verification value and delivering them to the control unit 30 as the utilization history.

With respect to the history ud delivered from the history creating unit 31, the utilization-value creating unit 20 performs the process of calculating the following Hash value,

$$Hu = \text{Hash}(ud) \quad [\text{Numerical Formula 3}]$$

and storing the calculated result in the utilization-value holding unit 21, which holds the verification value at that point of time.

As in Embodiment 1 of the present invention, the digital signature unit 24 uses the private key held in the token private key holding unit 23 holding the special private key for the token to provide the digital signature with respect to the value given. According to this embodiment of the invention, further, the signature verification unit 34 is provided so as

to verify whether the signature delivered by the use of the public key of the center held in the center public-key holding unit 33 is the signature of the center. Digital signature technology such as RSA signature is basically usable for these constituent units; however, the detailed description thereof will be omitted as it is well known technology.

Fig. 17 shows the construction of the information processing unit 11 according to this embodiment of the invention, wherein like reference characters designate like or corresponding parts of Fig. 2. As shown in Fig. 17, though the construction is substantially similar to what is shown in Embodiment 1 of the present invention, the token enters the halt mode at a certain point of time in the information processing unit 11 according to this embodiment of the invention and in order to make the function restart, a history has to be transmitted to the center to cause the center to send the restart message accordingly. Therefore, a verification value reception unit 36 for receiving a verification value with a signature from the center is slightly varied. Further, the history held in the history holding unit 16 is also different in construction.

Fig. 18 shows the construction of the recovery unit 13 of the center according to this embodiment of the invention, wherein like reference characters designate like or corresponding parts of Fig. 5. In comparison with the constitution of Embodiment 1 of the present invention, since the verification value with the signature has to be sent to the information processing unit 11 when the correctness of a history is verified, there are additionally installed constituent units for the purpose; namely, a center private-key holding unit 37, a digital signature unit 38 and a verification-value-with-signature transmitting unit 39. As the utilization history sent from the information processing unit 11 is different in construction, the history processed in the recovery center naturally differs.

Figs. 19A to 19E show the construction of the utilization history held in each of the constituent units.

Fig. 19A refers to the utilization history recorded in the history holding unit 16 of the information processing unit 11. The contents of the individual history include two: a pair of information identifier shown in Fig. 19C and verification value held in the token at that point of time.

When the history is sent from the information processing unit 11 to the center, the verification value with the signature of the token is affixed to the last position of the line of the history shown in Fig. 19B. The verification value with the signature is output when the token 12 ceases to function and the token 12 provides the verification value with the signature at that point of time shown in Fig. 19D.

The center employs the verification value with the signature for verifying the history shown in Fig. 19D. When the correctness is proved as a result of verification, the center provides the verification value attached to the last position as a message for restarting the function of the token 12 with a signature and the value thus obtained is sent to the information processing unit 11. This is shown in Fig. 19E.

The processing performed by the recovery unit 13 will subsequently be described. When a history is transmitted from the information processing unit 11, it is received by the history reception unit 25. The history received is stored in the history holding unit 26 and also delivered to the signature verification unit 29. The signature verification unit 29 selects the public key of the token 12 connected to the information processing unit 11 which has transmitted the history from among the plurality of token public keys stored in the token public-key holding unit 28, and verifies the signature of the history using the public key. The verified result is held together with the history stored in the history holding unit 26.

When the reception of the history is completed, the history verification unit 27 starts operating. The history verification unit 27 refers to not only the history received now but also the result of verifying the signature affixed thereto. If the result of verifying the signature is incorrect, processing thereafter is not performed. If the result of verifying the signature is correct, it is further verified whether the contents of the signature are correct.

The process of verifying the contents of the signature is performed as follows:

(1) It is assumed that the line of the history sent is as follows:

(id₁, hu₀), (id₂, hu₁), (id₃, hu₂), ..., (id_n, hu_{n-1}), sign (hu_n) where id = information identifier, hu = verification value at a point of time the history is created, and sign () = sign of the token.

(2) The verification value sent by the token previously is found out of the history holding unit and defined as Hould.

(3) The verification value hu₀ is taken out of the initial history (ID₁, hu₀) of the utilization history that has been sent to make it certain whether the verification value is equal to Hould.

(4) Subsequently, (ID₁, hu₀) is calculated to make it certain whether the (ID₁, hu₀) conforms to hu₁.

(5) This step is repeatedly taken up to the final verification value hu_n likewise.

(6) On condition that the utilization history has passed every inspection, it is regarded as being correct.

Only when the history is judged correct through the verification process, the final verification value hu_n is sent to the signature verification unit, so that a digital signature is provided by means of the public key of the center. Then the verification value with the signature of the center is sent back to the information processing unit from which the history has been transferred.

With the arrangement above, since the function of the token is stopped at a certain point of time, the user of the information processing unit has to send a correct history to the center in order to restart the function of the token. Therefore, the user can be urged to recover the history.

Since the final verification value is recorded on the center side, verification is proved to be simply unsuccessful even in a case where the correct history sent from the token is partially destroyed for some reason or other; consequently, no change is caused to the data held on the center side. Therefore, normal verification is carried out by making the token send the history again.

Even when part of the history is destroyed (or lost), almost all the rest may be made verifiable at the time the history is verified by causing the token to output the verification value autonomously.

More specifically, not only when the user demands a verification value as described above but also when the load of the token is low, the token is allowed to output autonomously the verification value with the signature it holds at that point of time, so that even when part of the history is destroyed (or lost), almost all the rest becomes verifiable at the time the history is verified.

In this case, the utilization history sent to the center is constructed as shown in Fig. 20, for example. At this time, it is assumed that a history 25 has been lost by accident on the information processing unit side.

In the case of a utilization history having the verification value shown above at only the last position, the verification of a history 26 and thereafter is possible. Notwithstanding the fact that the contents of from histories 1 - 24 have not been lost, their correctness remains unverifiable.

When the history 25 is lost, only a history 24 becomes unverifiable and the remaining histories are made verifiable by inserting verification values with signatures halfway throughout. More specifically, histories from 1 to 10 are made verifiable by a verification value 1 with a signature; histories from 11 to 23 by a verification value 2 with a signature; histories from 25 to 36 by a verification value 3 with a signature; and histories from 37 to 57 by a verification value 4 with a signature.

Thus, most of the remaining histories are made verifiable even when part of any history is lost by inserting verification values among the histories at suitable intervals.

In order to materialize the arrangement above, a decision unit for deciding whether the load is low is provided in the control unit within the token and when the load of the token is low, it is only needed to autonomously create the verification value with the signature.

Moreover, it may be arranged that the verification value with the signature is output by the information processing unit, that is, in compliance with a request from the user unless the token does the operation autonomously. Consequently, the processing may be altered from not causing the node C (Step S64) of Fig. 14 to branch off from the node C of Fig. 16 but creating a verification value with a signature by updating the verification value and returning the verification value to the information processing unit 11.

Further, time information as the utilization history is made retrievable by letting the token have the clock function, whereby the recovery center can be informed of not solely the history about which information has been utilized but also the time when the information is used. The clock unit has an ordinary clock function and should only function as what outputs the present time in accordance with the request made by holding the date including years, months and days, and the time. In order to include the time in the history, it is only needed to couple the time information to the information identifier. With the provision of the clock function, "the time passed after the preceding halt" can be set as the condition of restoring the above-described halt mode.

Although a history to be output outside is provided with the verification value held thereby at that point of time according to this embodiment of the invention, a count instead of the verification value may be output when the history is output outside by providing a counter unit in the token so that the count is counted each time the history is output. In this case, the portion as the hash function input described until now makes a utilization history and the count held at that point of time.

As set forth above, according to the present invention, data is not stored in the protective apparatus to reduce the quantity of held data but output outside the protective apparatus, and a verification value having a small quantity of data is to be stored instead. Consequently, the storage capacity and the necessary processing capabilities of the protective apparatus can be suppressed. Since the verification value is sent outside together with a signature, dishonest alteration is preventable to ensure that data is verified. Moreover, even though data are dispersed for storage, the order of data is restored to facilitate data verification by adding order-restoring information to the data to make the order of such data restorable. Since the relevant processing is made continuously performable when the protective apparatus receives a value resulting from providing the signature of a right person for the data held by the protective apparatus, the processing is made possible only by sending the data held in the protective apparatus to the right person and then sending back the data therefrom. Therefore, verification data is sent to the right person at all times to ensure that the verification data is recovered. Even though part of the data is destroyed or the like, most of the remaining data can be verified for certain by outputting the verification value with the signature frequently.

The foregoing description of a preferred embodiment of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. The embodiment was chosen and described in order to explain the principles of the invention and its practical applica-

tion to enable one skilled in the art to utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto, and their equivalents.

5 Claims

1. A data verifying method, comprising the steps of:

10 creating a verification value of a data body inside a protective apparatus from a verification value of the relevant data body out of a plurality of data bodies generated in sequence and a verification value of a data body preceding the relevant data body;
 creating a verification value with a signature by adding a digital signature inside the protective apparatus to the verification value created for the last data body out of the plurality of data bodies tube verified at a time;
 15 sending the verification value with the signature outside from the protective apparatus; and
 verifying the plurality of data bodies based on the plurality of data bodies and the verification value with the signature.

2. An apparatus for creating data to be verified, said apparatus comprising:

20 means for generating data bodies in sequence;
 verification value storage means for storing verification values;
 verification value creation means for creating a new verification value from the verification value stored in the verification value storage means and a newly generated data body and updating the verification value stored in the verification value storage means to the new verification value; and
 25 signature means for attaching a signature to the verification value stored in the verification value storage means at predetermined timing;
 wherein said verification value creation means, said verification value storage means and said signature means are installed in a protective apparatus.

3. A data verifying apparatus, comprising:

a plurality of data bodies generated in sequence;
 means for receiving a verification value with a signature resulting from providing a signature for the verification value calculated from the plurality of data bodies;
 35 signature verifying means for verifying the signature on the verification value received; and
 verifying means for verifying the correctness of the plurality of data bodies received from the verification value with the signature verified by the signature verifying means.

4. A history holding method for holding in a protective apparatus only a verification value resulting from sequential calculations with respect to a group of history data comprising:

a plurality of continuous history data, and providing a signature for only the verification value when the verification value is output from the protective apparatus outside.

5. A history holding apparatus comprising:

data input means for inputting a plurality of continuous data;
 data processing means for processing the data;
 verification value creation means for creating a verification value with history data relevant to the data processing and the verification value held at this point of time as inputs;
 50 verification value holding means for holding the verification value thus created; and
 signature means for providing a signature for the verification value;
 wherein said verification value creation means, said verification value holding means and said signature means are at least installed in a protective apparatus.

6. A history holding apparatus as claimed in claim 5, wherein unidirectional functions are used for calculations applicable to said verification value creation means.

7. A history holding apparatus as claimed in claim 5, wherein the history data is in the form of a combination of the history data body and the verification value at the time the history data is processed.
- 5 8. A history holding apparatus as claimed in claim 5, further comprising counter means for counting each time data is processed, wherein the history data in the history data group is in the form of a combination of the count when the data is processed and a history body.
9. A history holding apparatus as claimed in claim 5, wherein the verification value with the signature is output in compliance with a user's request.
- 10 10. A history holding apparatus as claimed in claim 5, wherein the history holding means comprising a single CPU with software; and
wherein when the load of the CPU applied by the data processing means is low, the signature means creates and outputs the verification value with the proper signature.
- 15 11. A history holding apparatus as claimed in claim 5, further comprising function halt means for stopping the function of the data processing means at a point of time the verification value is output until a proper instruction is given from the outside.
- 20 12. A history holding apparatus as claimed in claim 11, further comprising halt condition holding means for stopping the function, wherein when the conditions described in the halt condition holding means are met, the function halt means outputs the verification value with the signature written thereto and stops its function.
- 25 13. A history holding apparatus as claimed in claim 11, further comprising proper public-key holding means for holding a public key of an external right person, wherein the function halt means verifies that an accepting instruction is intended to restore the function corresponding to the lastly-output verification value provided with a digital signature made by the external right person and that by verifying the signature with the public key held by the proper public-key holding means at the time of receiving the instruction, whether or not the verification value with the signature is equal to the verification value held by the verification value holding means.
- 30 14. A history verifying apparatus comprising:

data input means for inputting a verification value with a signature, the signature being provided for the verification value calculated from a plurality of continuous history data in group and from the data groups;
35 signature verifying means for verifying the signature of the verification value thus received with the signature; and
verifying means for verifying the correctness of the data group received from the data group received and the verification value whose signature has been verified.
- 40 15. A history verifying apparatus as claimed in claim 14, further comprising previous verification value storage means for storing the verification value received the last time;
wherein the verifying means employs the previous verification value when making verification.
- 45 16. A history verifying apparatus as claimed in claim 14, wherein the calculations for use in said verifying means are based on unidirectional functions.
17. A history verifying apparatus as claimed in claim 14, wherein the history data is in the form of a combination of the history data body and the verification value at the time the history data is processed.
- 50 18. A history verifying apparatus as claimed in claim 14, wherein the history data in the history data group is in the form of a combination of the value of the counter when the data is processed and a history body.
19. A history holding apparatus comprising:

55 data storage means for holding data;
halt condition holding means for holding predetermined conditions at the time the function is stopped;
function halt means for stopping the function when the conditions held in the halt condition holding means are met and keeping the function stopped until a proper instruction is received from the outside;

private-key holding means for holding a private key;

digital signature means for providing a digital signature using the private key held in the private-key holding means for the data group held in data holding means;

digital signature holding means for holding the digital signature affixed; and

proper public-key holding means for holding the public key of an external right person, wherein the function halt means verifies that an accepting instruction is intended to restore the function corresponding to the digital signature provided by the external right person for the digital signature held in the digital signature holding means and that by verifying the signature with the public key held by the proper public-key holding means at the time of receiving the instruction, whether or not the value with the signature is equal to the value held by the digital signature holding means.

20. An electronic equipment comprising:

function halt means for stopping at least part of the function of an electronic equipment body when predetermined conditions are met;

means for outputting predetermined data outside;

means for receiving data with a signature, the data being created by providing the signature for the predetermined data;

signature verifying means for verifying the signature with respect to the data with the signature; and

means for releasing the halt state of that part of the function when the correctness of the signature of the data with the signature is verified by the signature verifying means.

21. A computer program product for effecting interaction between a data creation apparatus and a data recovery apparatus for recovering data bodies that are output from the data creation apparatus, which comprises means for generating the data bodies in sequence, verification value holding means for holding verification values, verification value creation means for creating a new verification value from the verification value held in the verification value holding means and a newly generated data body and updating the verification value held in the verification value holding means to the new verification value, and signature means for attaching a signature to the verification value held in the verification value holding means at predetermined timing, characterized by causing a computer to take the steps of:

storing the data body that is output from the data creation apparatus and the verification value provided with the signature, and

sending the data body and the verification value with the signature thus stored therein to the data recovery apparatus at predetermined timing.

FIG.1

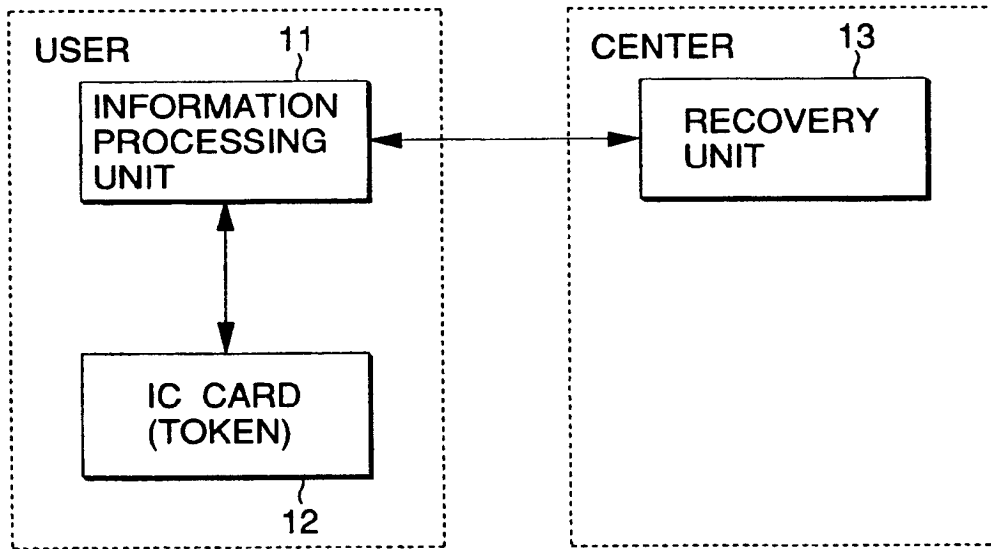


FIG.2

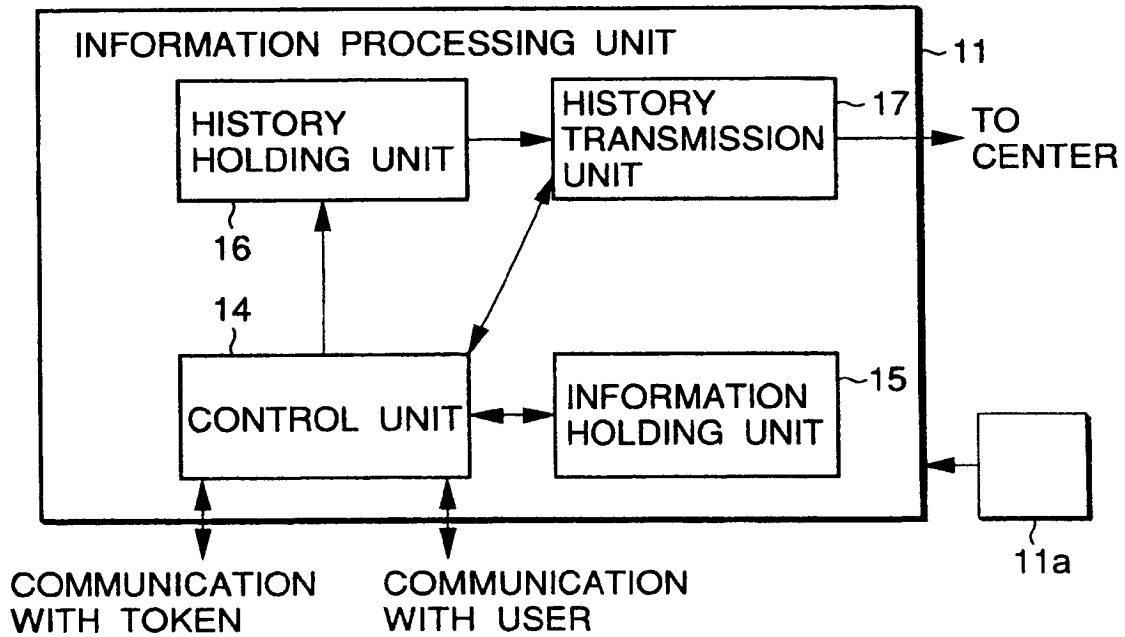


FIG.3

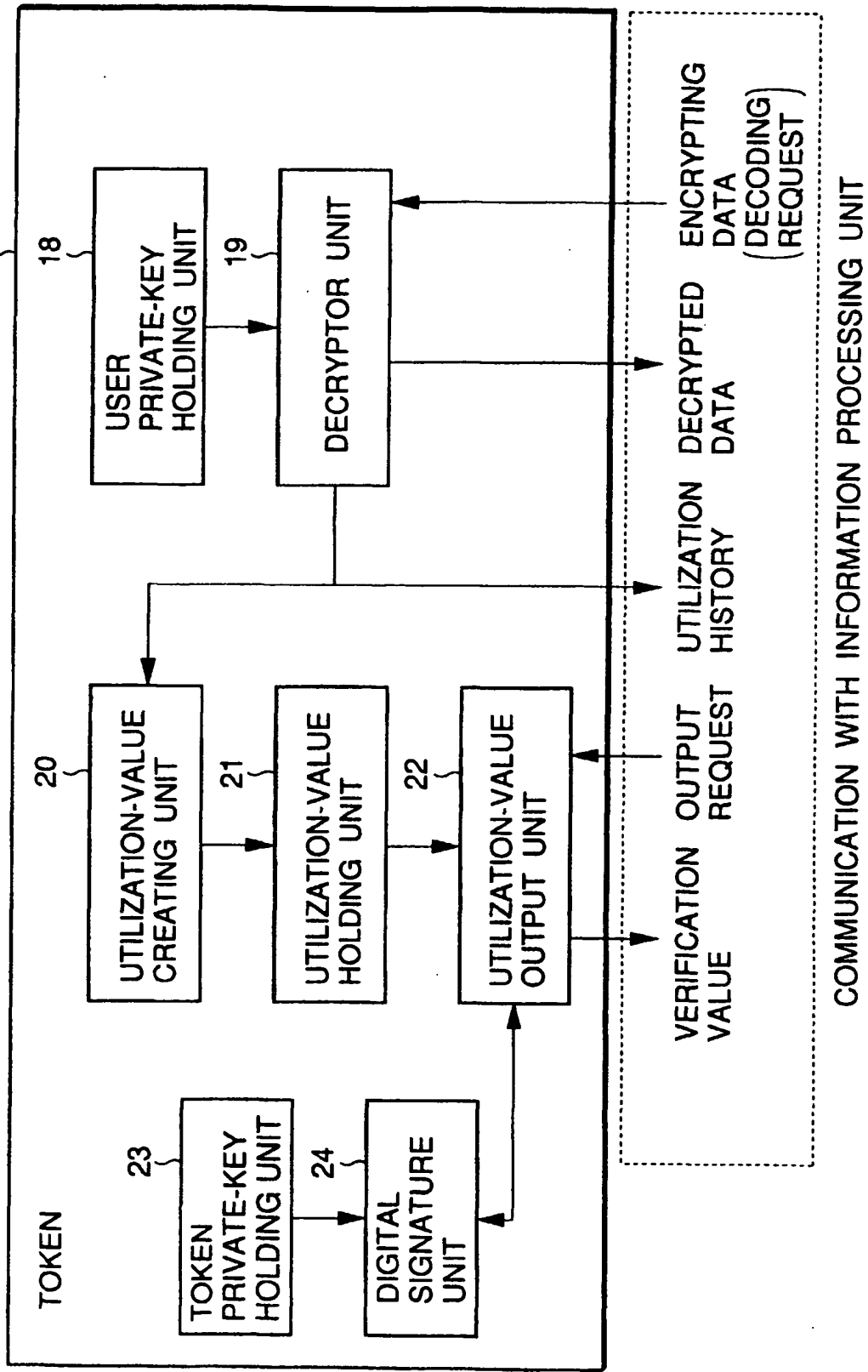


FIG.4

VERIFICATION VALUE
A092EF7B708B810098AFF89C046F8926

CONTENTS OF VERIFICATION-VALUE HOLDING UNIT

FIG.5

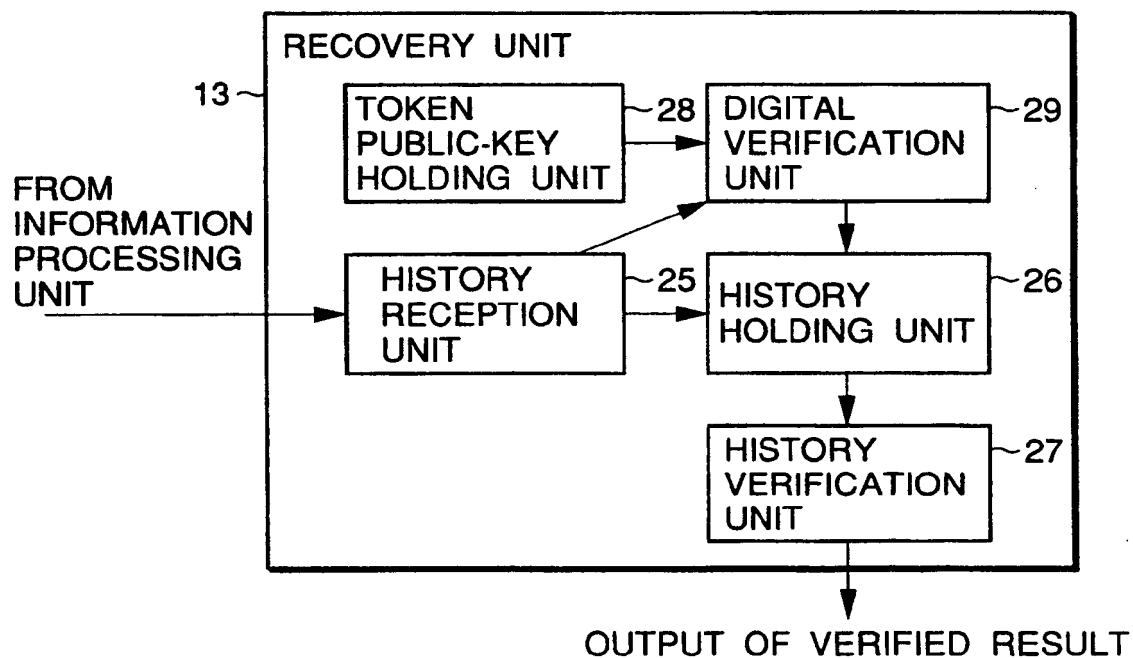
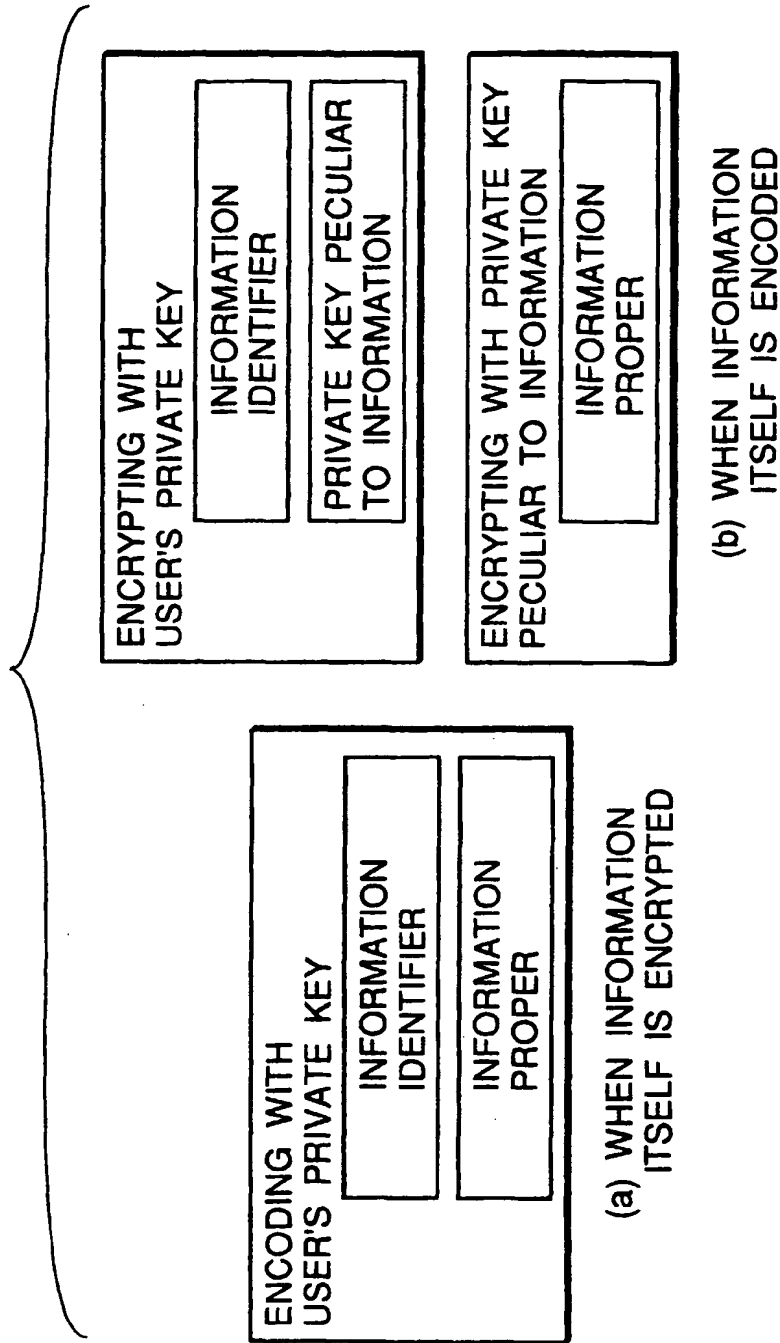


FIG.6



CONSTRUCTION OF ENCRYPTED INFORMATION

FIG.7A



UTILIZATION HISTORY RECORDED IN HISTORY HOLDING UNIT OF INFORMATION PROCESSING UNIT

FIG.7B

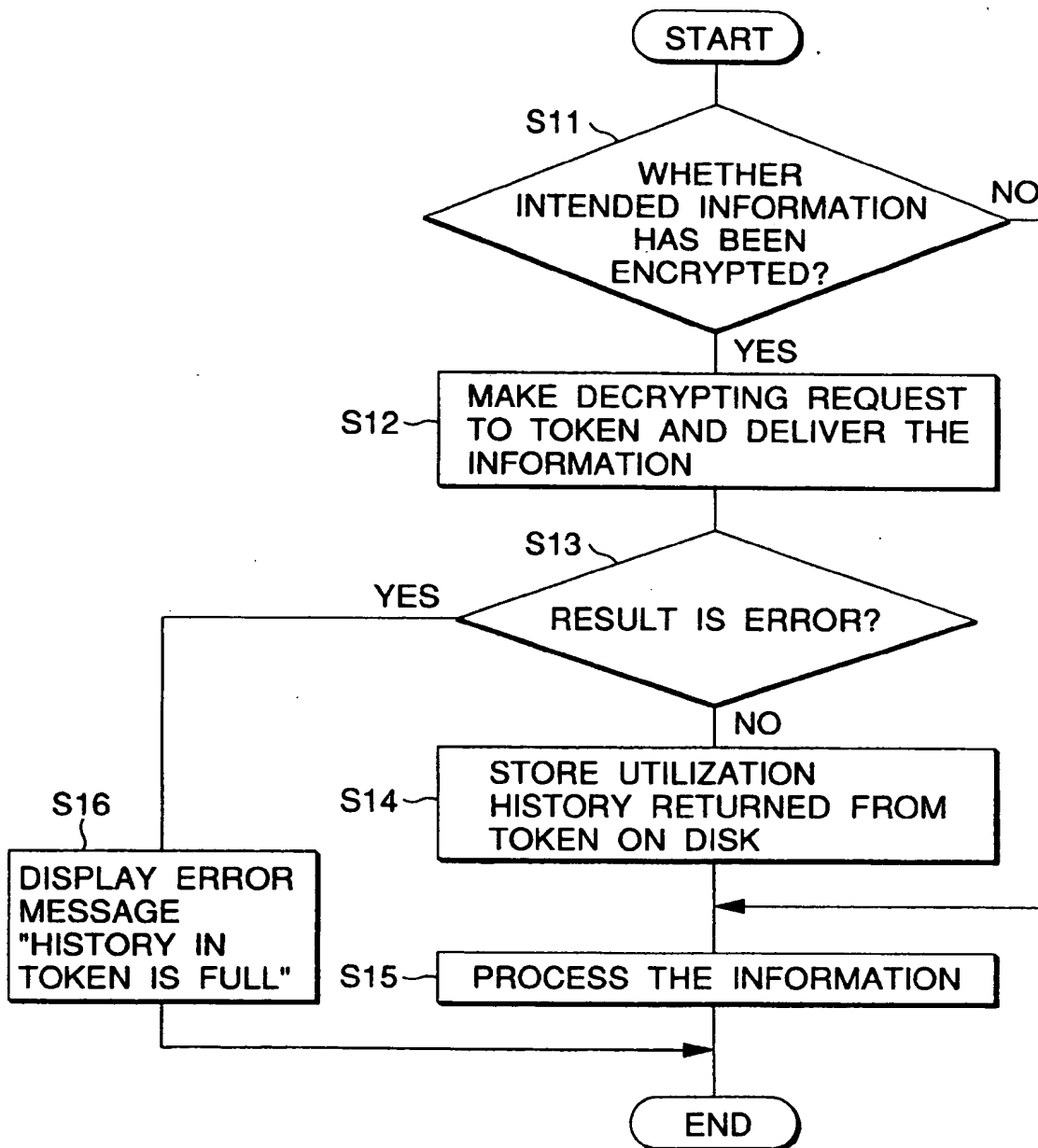


UTILIZATION HISTORY SENT FROM INFORMATION PROCESSING UNIT TO CENTER

CONSTRUCTION OF UTILIZATION HISTORY

FIG.8

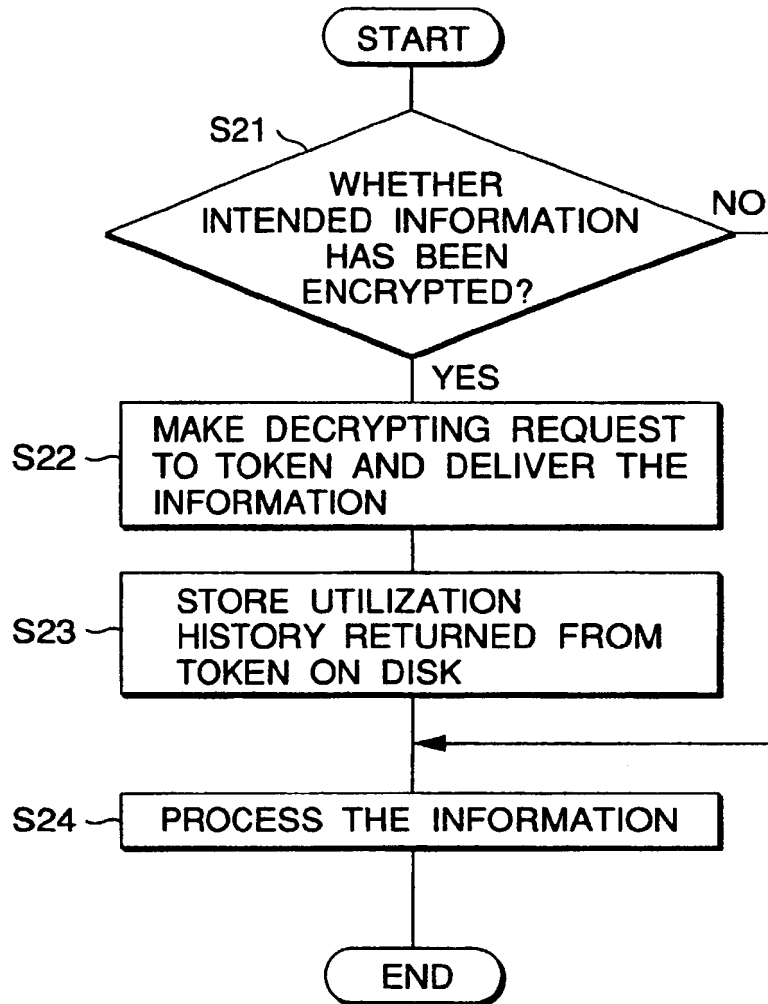
PROCESSING WHEN REQUEST FOR UTILIZING
INFORMATION IS RECEIVED FROM USER



PROCESSING IN CONTROL UNIT OF
INFORMATION PROCESSING UNIT

FIG.9

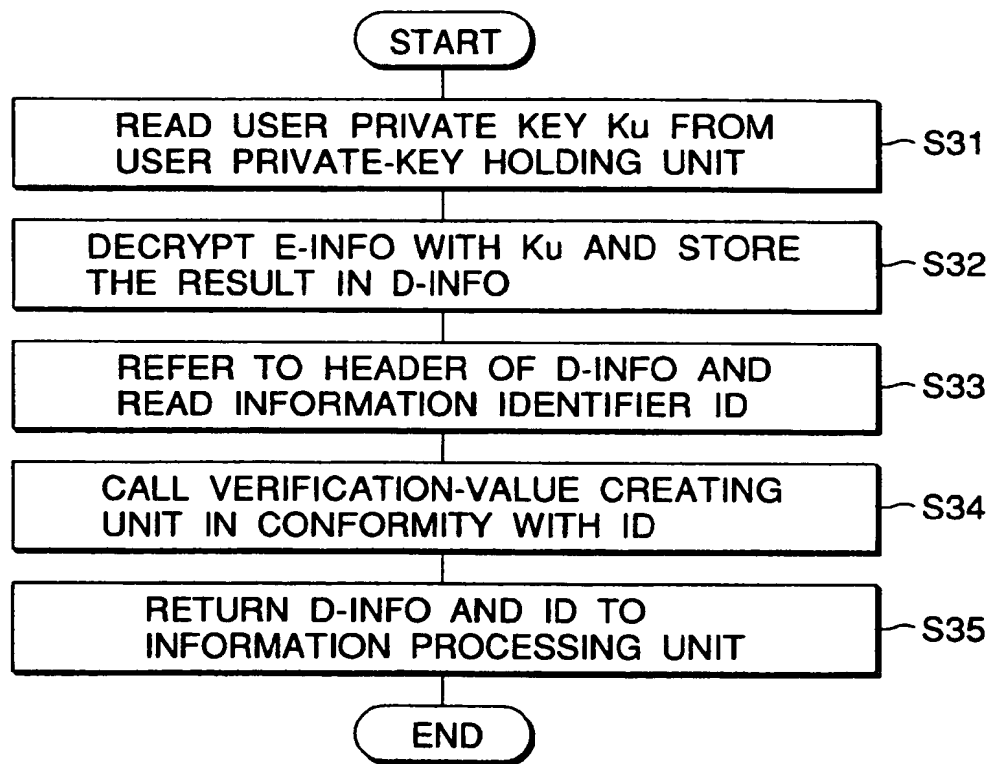
PROCESSING WHEN UTILIZATION HISTORY
RECOVERY INSTRUCTION IS RECEIVED FROM USER



PROCESSING IN CONTROL UNIT OF
INFORMATION PROCESSING UNIT

FIG.10

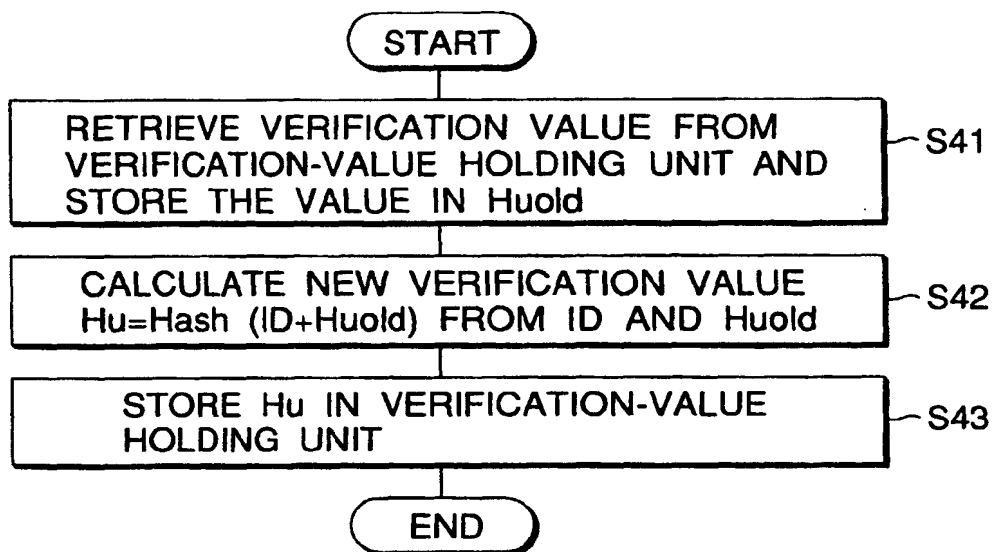
PROCESSING WHEN REQUEST FOR DECRYPTING
ENCRYPTED INFORMATION E-INFO IS RECEIVED
FROM INFORMATION PROCESSING UNIT



PROCESSING IN DECRYPTING UNIT OF TOKEN

FIG.11

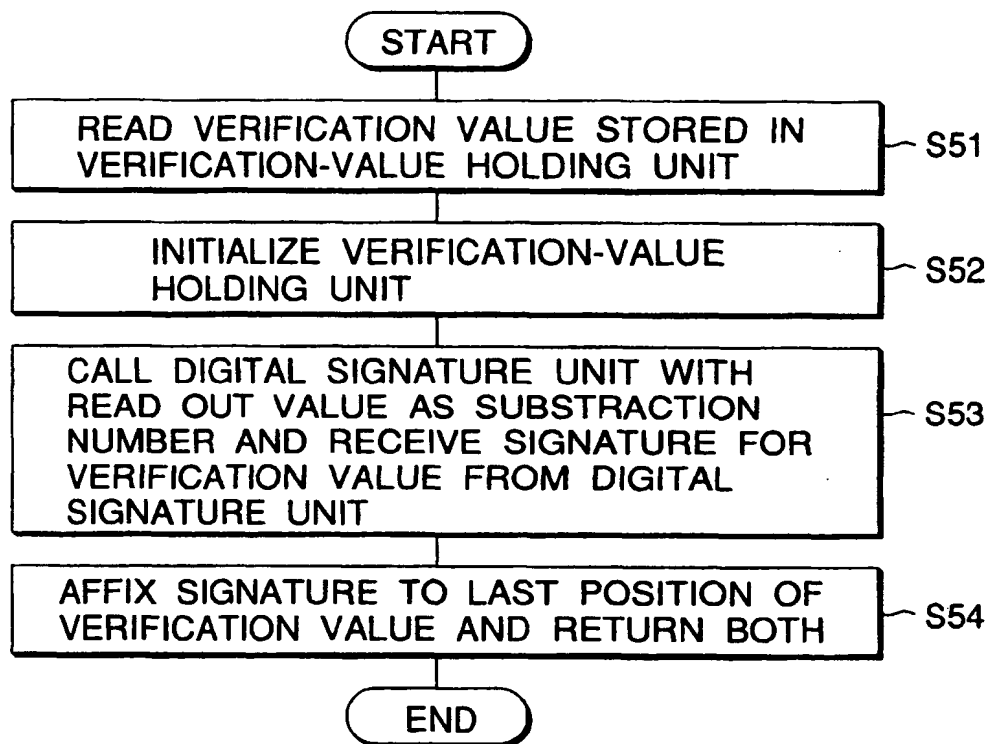
PROCESSING WHEN INFORMATION IDENTIFIER ID IS
DELIVERED AND CALLED FROM DECRYPTING UNIT



PROCESSING IN VERIFICATION-VALUE
CREATING UNIT OF TOKEN

FIG.12

PROCESSING WHEN VERIFICATION-VALUE
OUTPUT REQUEST IS RECEIVED FROM
INFORMATION PROCESSING UNIT



PROCESSING IN VERIFICATION-VALUE
OUTPUT UNIT OF TOKEN

FIG.13

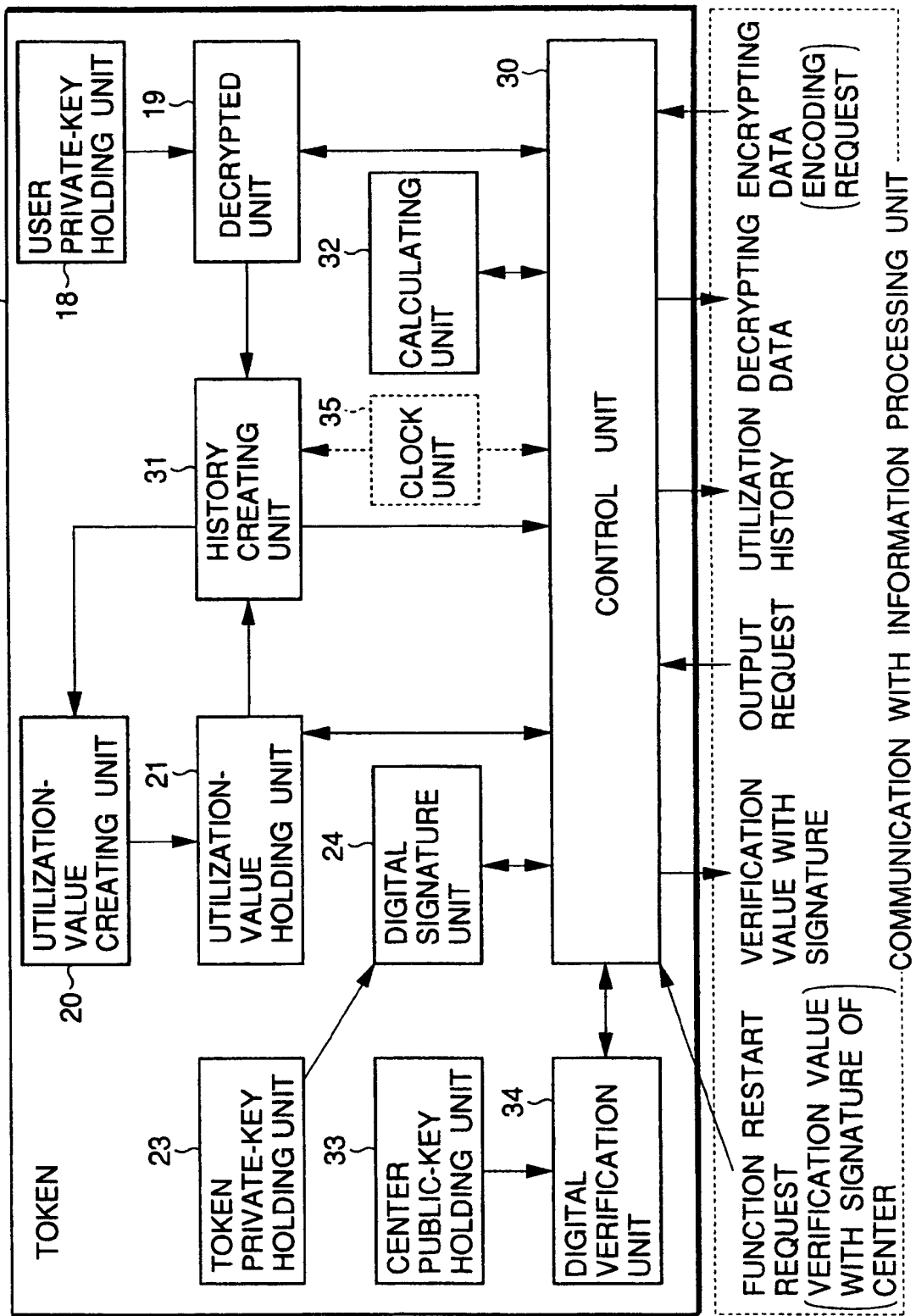


FIG.14

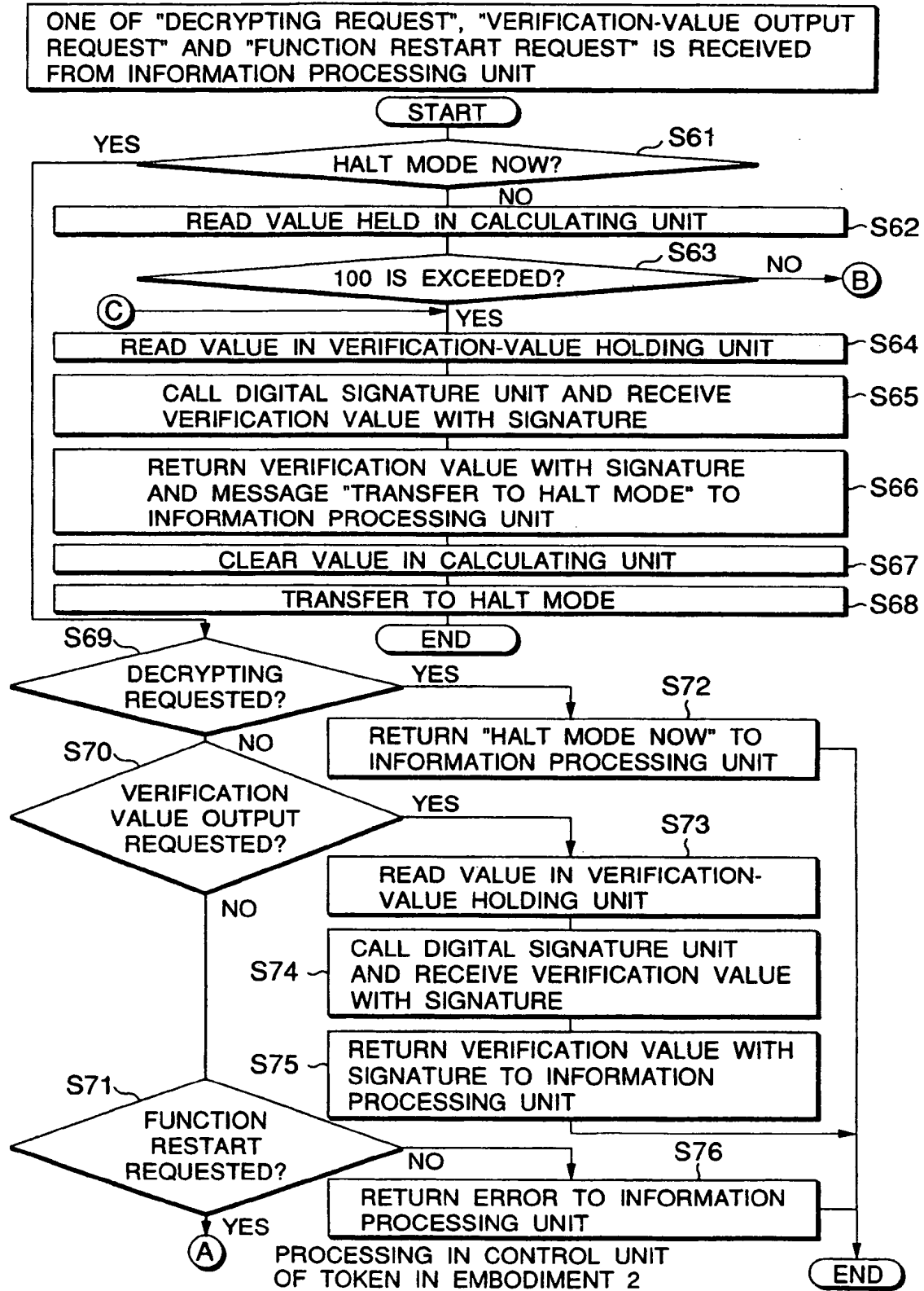
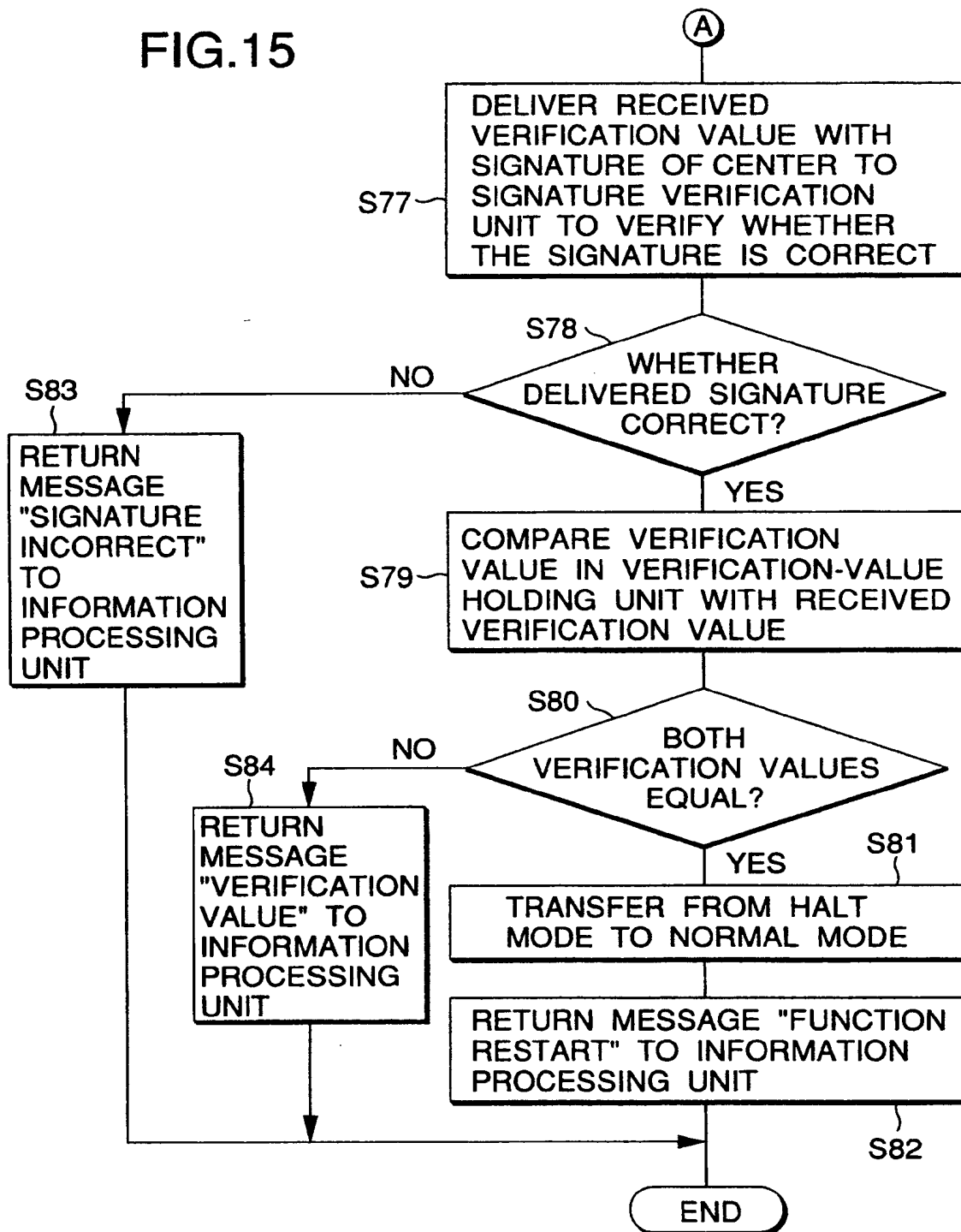
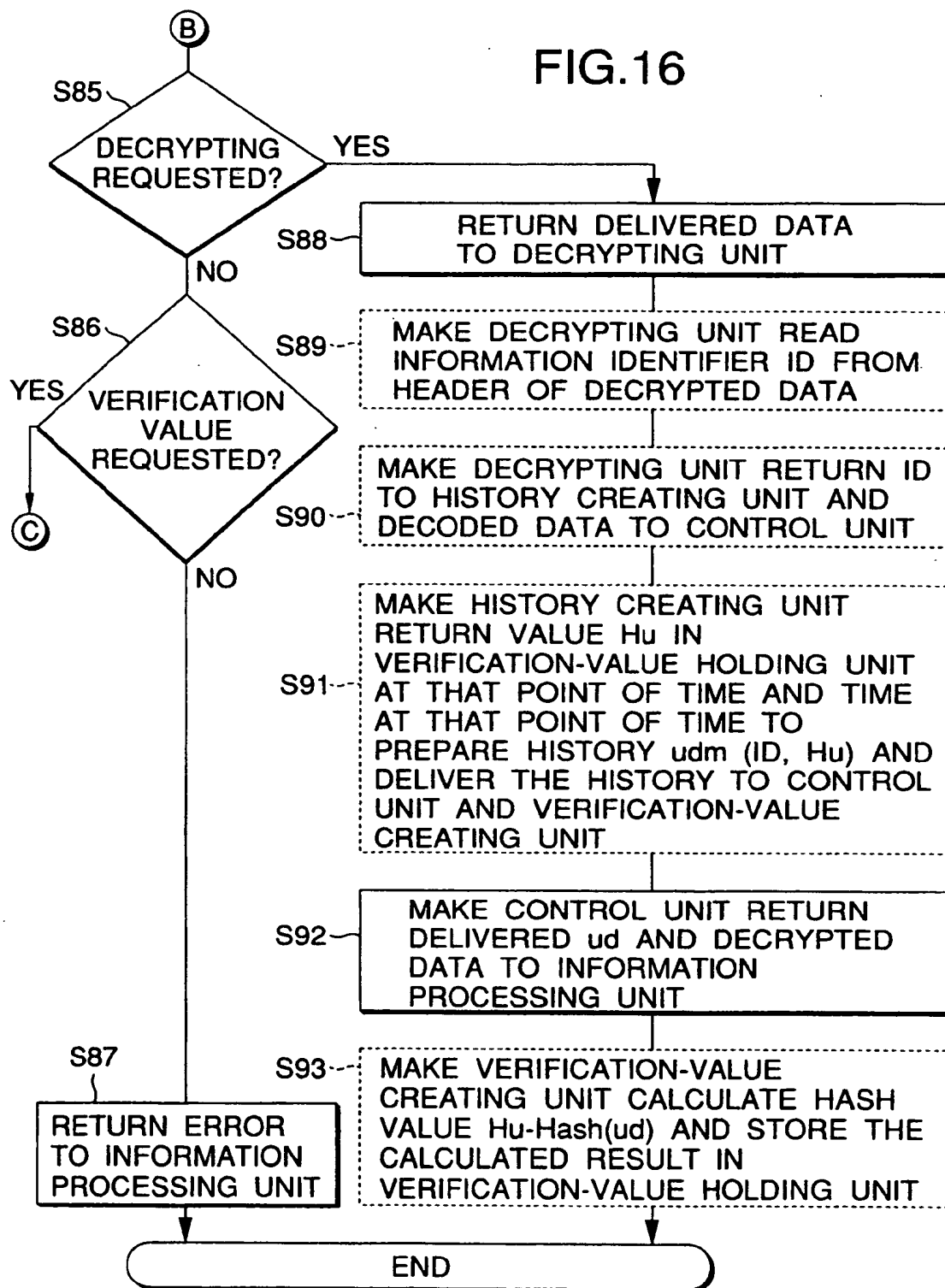


FIG.15



PROCESSING IN CONTROL UNIT
OF TOKEN IN EMBODIMENT 2

FIG.16



PROCESSING IN CONTROL UNIT
OF TOKEN IN EMBODIMENT 2

FIG.17

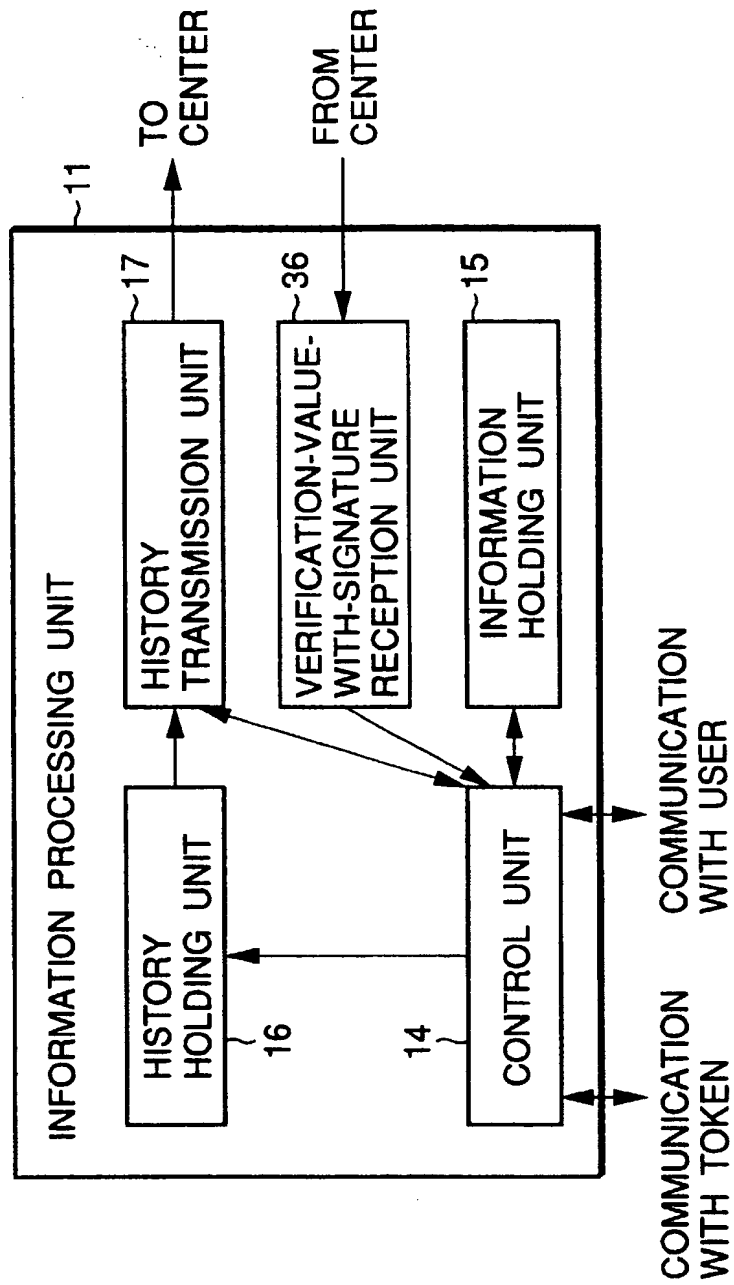


FIG.18

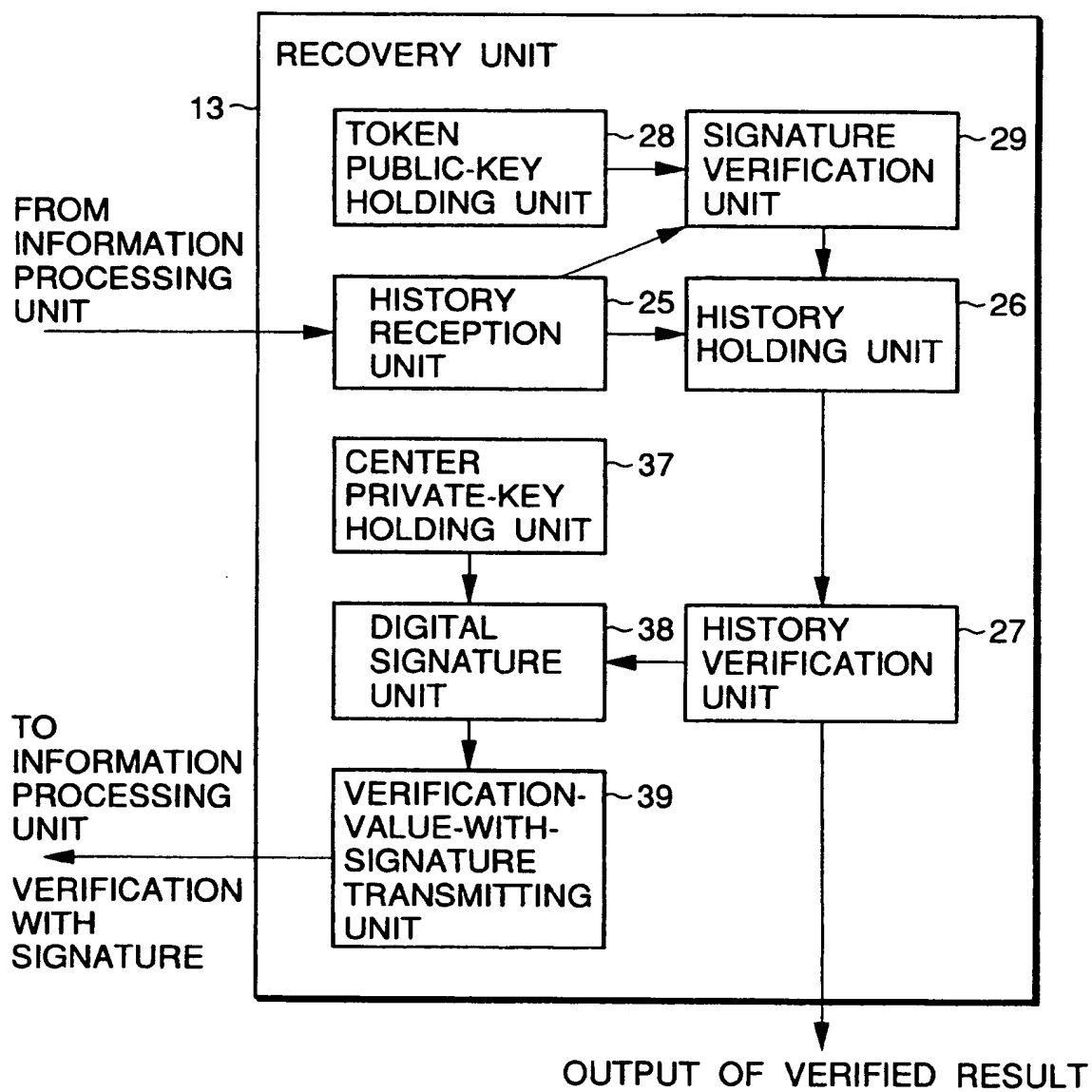
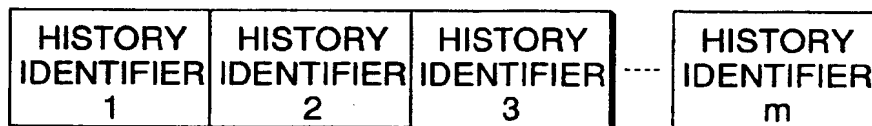


FIG.19A



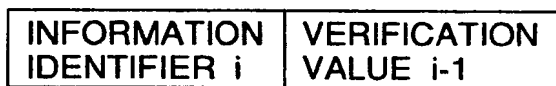
UTILIZATION HISTORY RECORDED IN HISTORY
HOLDING UNIT OF INFORMATION PROCESSING UNIT

FIG.19B



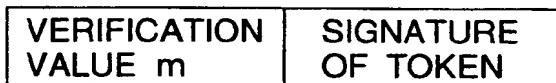
UTILIZATION HISTORY SENT FROM
INFORMATION PROCESSING UNIT TO CENTER

FIG.19C



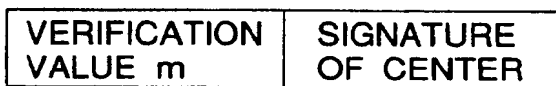
CONTENTS OF NO.i UTILIZATION HISTORY

FIG.19D



CONTENTS OF VERIFICATION VALUE WITH SIGNATURE

FIG.19E



MESSAGE SENT FROM CENTER TO USER

CONSTRUCTION OF UTILIZATION HISTORY AND
VERIFICATION VALUE IN EMBODIMENT 2

FIG.20

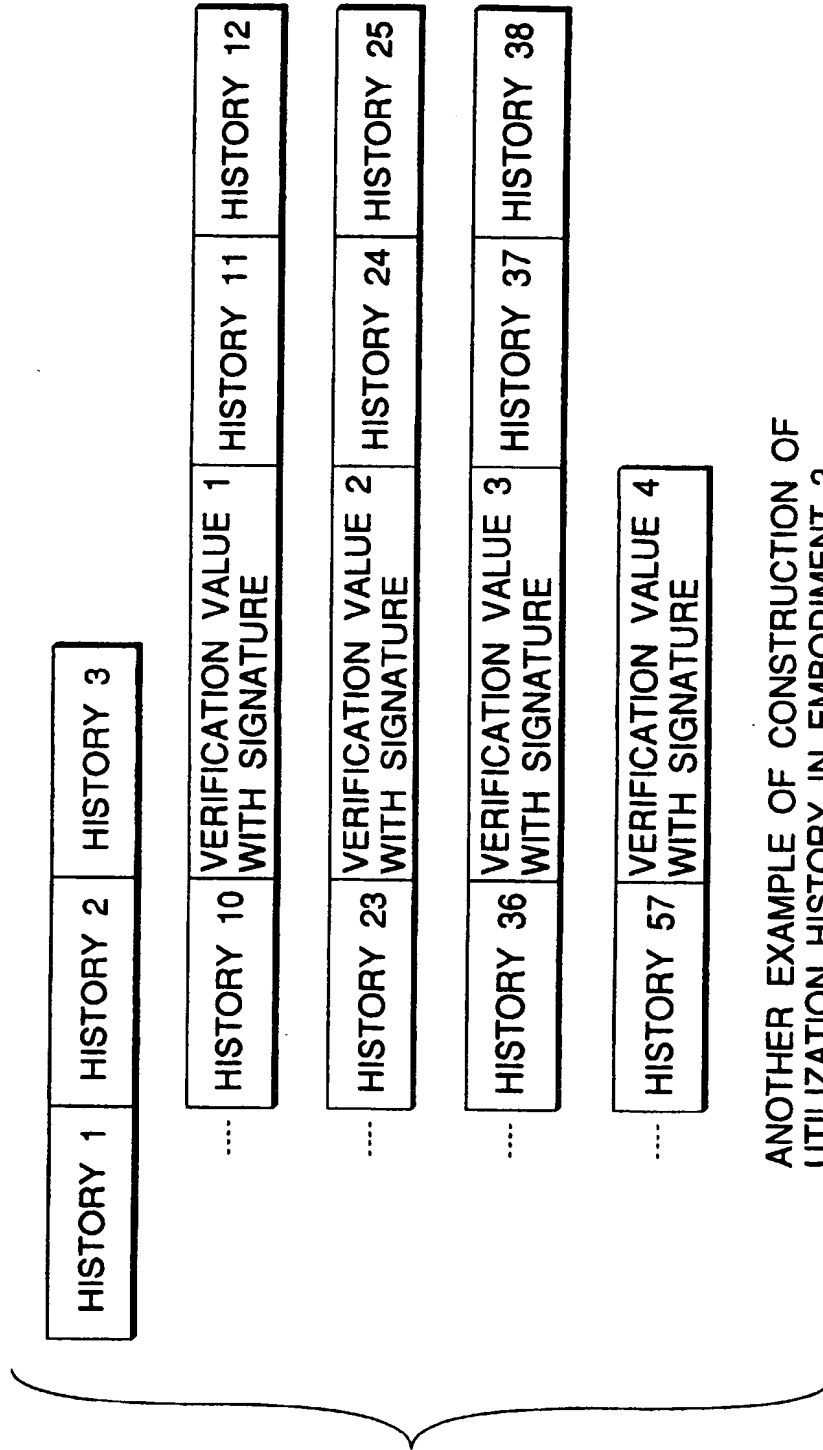
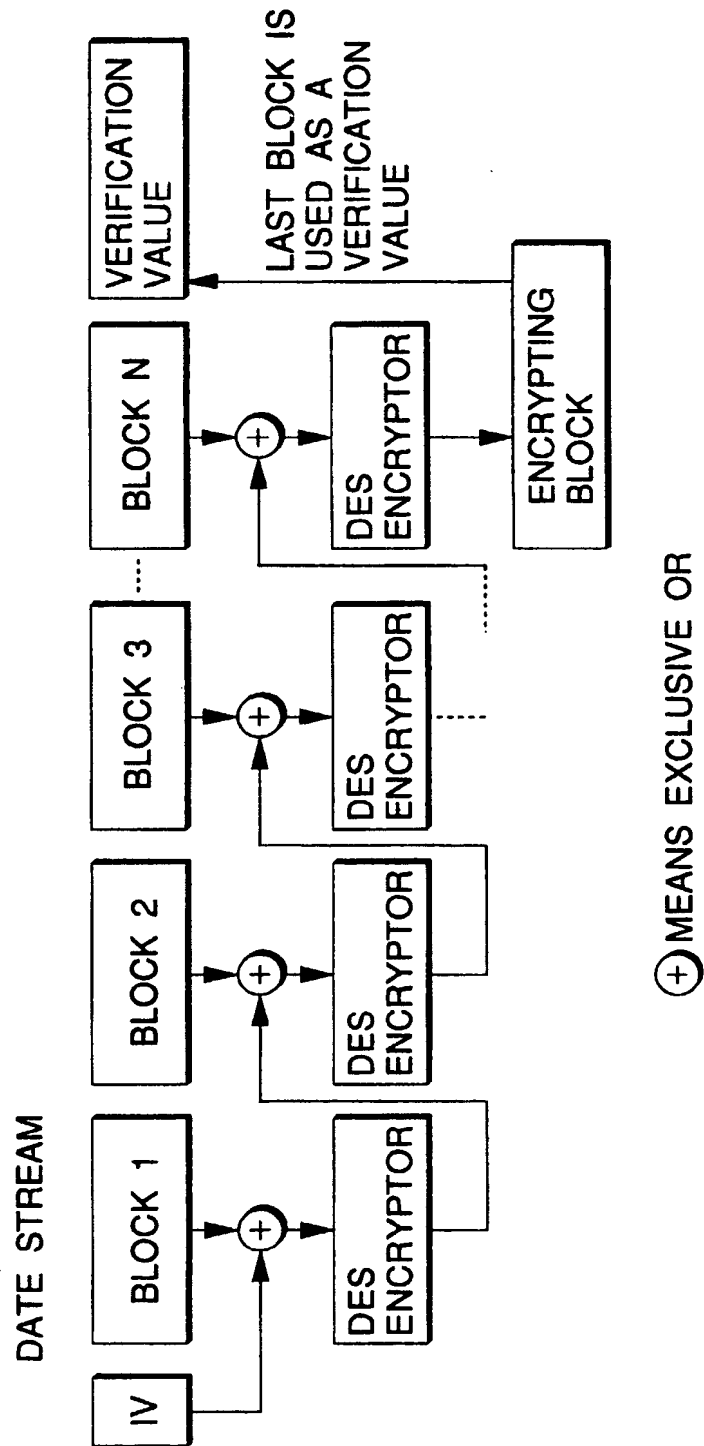
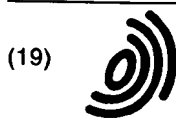


FIG.21



CONSTRUCTION OF DES-MAC



(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
28.07.2004 Bulletin 2004/31

(51) Int Cl.7: **G06F 1/00**

(43) Date of publication A2:
22.04.1998 Bulletin 1998/17

(21) Application number: **97118074.0**

(22) Date of filing: **17.10.1997**

(84) Designated Contracting States:
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE**
Designated Extension States:
AL LT LV RO SI

(30) Priority: **21.10.1996 JP 27842396**

(71) Applicant: **FUJI XEROX CO., LTD.**
Minato-ku, Tokyo (JP)

(72) Inventors:
• **Saito, Kazuo, c/o Fuji Xerox Co.,Ltd.**
Ashigarakami-gun, Kanagawa (JP)
• **Shin, Kilho, c/o Fuji Xerox Co.,Ltd.**
Ashigarakami-gun, Kanagawa (JP)
• **Takeda, Koji, c/o Fuji Xerox Co.,Ltd.**
Ashigarakami-gun, Kanagawa (JP)

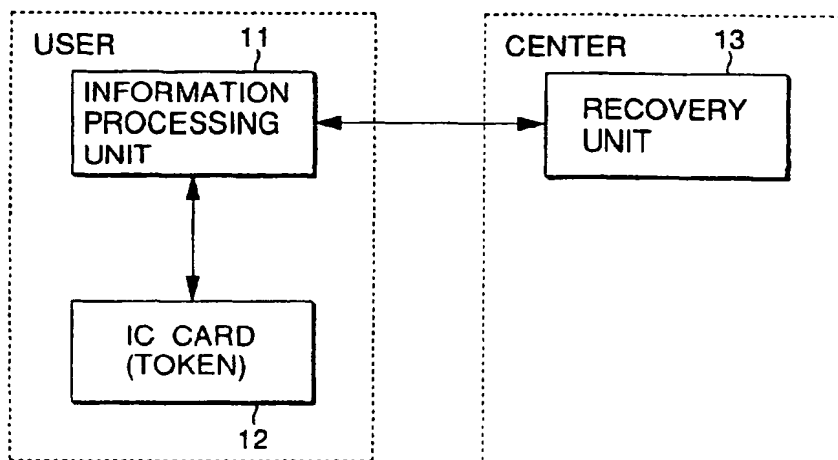
(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) **Method and apparatus for data verification**

(57) A token 12 creates utilization history information and sends the information to an information processing unit 11 and simultaneously creates a verification value and stores the value in a utilization-value holding unit 21. The information processing unit 11 records the utilization history information in a history holding unit 16. On receiving a verification-value output request from the information processing unit 11, the to-

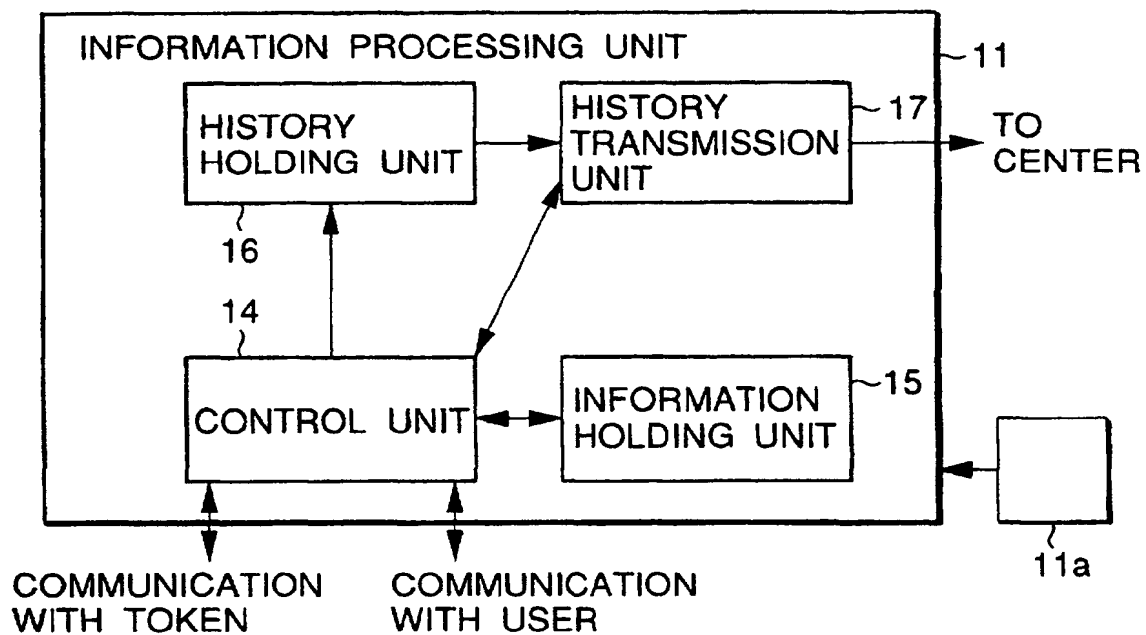
ken 12 provides the verification value with a signature and outputs the combination of the verification value and the signature. The information processing unit sends to a recovery unit 13 the verification value with the signature as well as the utilization history information. The recovery unit 13 verifies the signature and also the utilization history on the basis of the verification value further.

FIG.1



EP 0 837 383 A3

FIG.2





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 11 8074

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
E	WO 97/19537 A (WALKER ASSET MANAGEMENT L P) 29 May 1997 (1997-05-29) * abstract * * page 1, line 5 - line 9 * * page 1, line 31 - page 2, line 5 * * page 7, line 30 - page 8, line 20 * * page 11, line 1 - line 31 * * page 12, line 3 - line 4 * * page 19, line 19 - page 21, line 26 * * page 24, line 4 - line 23 * * page 79, line 10 - page 86, line 1 * * page 89, line 25 - line 30 * * page 91, line 1 - page 97, line 10 * * page 102, line 10 - page 104, line 2 * * page 111, line 7 - page 112, line 20 * * page 116, line 9 - page 117, line 1 * * page 118, line 28 - page 120, line 7 * * page 132, line 10 - line 31 * * page 136, line 13 - page 137, line 23 * -----	1-18,21	G06F1/00
A	BRUCE SCHNEIER: "Applied Cryptography, protocols, algorithms and source code in C" 1994, JOHN WILEY & SONS, U.S., XP002250692 * page 33 - page 35 * * page 157 - page 158 * -----	1,2,4,21	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G06F H04L
A	US 5 377 268 A (HUNTER KEVIN D) 27 December 1994 (1994-12-27) * abstract * -----	1-18,21	
-/--			
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 6 May 2004	Examiner Anticoli, C
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03.82 (P04C01)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 11 8074

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	MORI R ET AL: "SUPERDISTRIBUTION: THE CONCEPT AND THE ARCHITECTURE" TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS OF JAPAN, INST. OF ELECTRONICS & COMMUNIC. ENGINEERS OF JAPAN. TOKYO, JP, vol. E73, no. 7, July 1990 (1990-07), pages 1133-1146, XP000159229 * page 1134, column 1, line 36 - column 2, line 7 * * page 1135, column 1, line 31 - column 2, line 16 * * page 1136, column 1, line 16 - line 24 * * page 1136, column 1, line 42 - column 2, line 8 * * page 1138, column 2, line 10 - line 11 * -----	19,20	
A	US 5 258 906 A (KROLL MARK W ET AL) 2 November 1993 (1993-11-02) * abstract * * column 1, line 56 - column 2, line 68 * * column 6, line 33 - line 37 * -----	19,20	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 6 May 2004	Examiner Anticoli, C
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03 82 (P04C01)



European Patent
Office

Application Number

EP 97 11 8074

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

- ☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):
- ☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

- ☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.
- ☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.
- ☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:
- ☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:



European Patent
Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 97 11 8074

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-18, 21

generation and verification of data bodies created in a
sequence by creating verification values and attaching a
signature

2. claims: 19-20

stopping a function in an apparatus comprising means for
verifying an instruction intended to restore the function
using asymmetric signature techniques

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 97 11 8074

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-05-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9719537 A	29-05-1997	US 5768382 A	16-06-1998
		US 5970143 A	19-10-1999
		AU 1081997 A	11-06-1997
		EP 0862824 A1	09-09-1998
		JP 2001526550 T	18-12-2001
		WO 9719537 A1	29-05-1997
		US 2003177347 A1	18-09-2003
		US 2002010013 A1	24-01-2002
US 5377268 A	27-12-1994	US 5243654 A	07-09-1993
		CA 2063084 A1	19-09-1992
		DE 69219510 D1	12-06-1997
		DE 69219510 T2	02-10-1997
		EP 0504843 A2	23-09-1992
US 5258906 A	02-11-1993	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)
~~THIS PAGE BLANK (USPTO)~~